Docket No: 241983US2SRD

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Hirofumi MURATANI GAU:

SERIAL NO: New Application EXAMINER:

FILED: Herewith

FOR: DIGITAL WATERMARK EMBEDDING APPARATUS AND METHOD, AND DIGITAL WATERMARK ANALYSIS APPARATUS, METHOD AND PROGRAM

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §120**.

☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of **35 U.S.C. §119(e)**: **Application No.** **Date Filed**

■ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY	APPLICATION NUMBER	MONTH/DAY/YEAR
Japan	2002-248941	August 28, 2002

Certified copies of the corresponding Convention Application(s)

■ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

☐ were filed in prior application Serial No. filed

☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

☐ (B) Application Serial No.(s)

☐ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Marvin J. Spivak
Registration No. 24,913

C. Irvin McClelland
Registration Number 21,124

22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

035098

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年　８月２８日

出願番号
Application Number: 特願２００２－２４８９４１

[ST.10/C]: [ＪＰ２００２－２４８９４１]

出願人
Applicant(s): 株式会社東芝

２００３年　１月３１日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３００２７９４

【書類名】　特許願

【整理番号】　A000202036

【提出日】　平成14年 8月28日

【あて先】　特許庁長官　殿

【国際特許分類】　G06F 15/00

【発明の名称】　電子透かし埋め込み装置、電子透かし解析装置、電子透かし埋め込み方法、電子透かし解析方法及びプログラム

【請求項の数】　26

【発明者】

【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

【氏名】　村谷　博文

【特許出願人】

【識別番号】　000003078

【氏名又は名称】　株式会社　東芝

【代理人】

【識別番号】　100058479

【弁理士】

【氏名又は名称】　鈴江　武彦

【電話番号】　03-3502-3181

【選任した代理人】

【識別番号】　100084618

【弁理士】

【氏名又は名称】　村松　貞男

【選任した代理人】

【識別番号】　100068814

【弁理士】

【氏名又は名称】　坪井　淳

【選任した代理人】

【識別番号】　100092196

【弁理士】

【氏名又は名称】　橋本　良郎

【選任した代理人】

【識別番号】　100091351

【弁理士】

【氏名又は名称】　河野　哲

【選任した代理人】

【識別番号】　100088683

【弁理士】

【氏名又は名称】　中村　誠

【選任した代理人】

【識別番号】　100070437

【弁理士】

【氏名又は名称】　河井　将次

【手数料の表示】

【予納台帳番号】　011567

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　電子透かし埋め込み装置、電子透かし解析装置、電子透かし埋め込み方法、電子透かし解析方法及びプログラム

【特許請求の範囲】

【請求項１】

デジタルコンテンツの複製物に電子透かしとして埋め込むべき識別情報に一意に対応する、序列を持った複数のシンボルの並びからなるシンボル列を生成する第１の生成手段と、

生成された前記シンボル列を構成する個々の序列のシンボルごとに、対応する埋め込み符号をそれぞれ生成する第２の生成手段と、

生成された前記個々の序列のシンボルにそれぞれ対応する埋め込み符号を、前記デジタルコンテンツの複製物に電子透かしとして埋め込む符号埋め込み手段とを備えたことを特徴とする電子透かし埋め込み装置。

【請求項２】

前記第２の生成手段は、前記シンボル列の個々の序列において、同一の序列に属する互いに異なるシンボルに対応する埋め込み符号同士が、相互相関の無い又は小さい乱数列になるように、前記埋め込み符号を生成することを特徴とする請求項１に記載の電子透かし埋め込み装置。

【請求項３】

前記第２の生成手段は、前記シンボル列の異なる序列に属するシンボルに対応する埋め込み符号同士についても、相互相関の無い又は小さい乱数列になるように、前記埋め込み符号を生成することを特徴とする請求項２に記載の電子透かし埋め込み装置。

【請求項４】

前記識別情報は、整数値であり、

前記シンボル列の各序列ごとに対応して特定の整数値が予め定められており、

前記第１の生成手段は、前記識別情報を前記シンボル列の個々の序列に対応する前記整数値でそれぞれ除し、これによって得られた個々の序列に対応する剰余値を当該序列に従って並べたものを、生成すべきシンボル列とすることを特徴と

する請求項１に記載の電子透かし埋め込み装置。

【請求項５】

前記識別情報は、整数値であり、

前記シンボル列の各序列ごとに対応して特定の整数値が予め定められており、

前記第１の生成手段は、前記識別情報を前記シンボル列の個々の序列に対応する前記整数値でそれぞれ除し、これによって得られた個々の序列に対応する剰余値をそれぞれ一意に対応する情報に変換し、これによって得られた個々の序列に対応する情報を当該序列に従って並べたものを、生成すべきシンボル列とすることを特徴とする請求項１に記載の電子透かし埋め込み装置。

【請求項６】

前記シンボル列の各序列ごとに対応して予め定められた特定の整数値は、互いに素の関係にある整数値であることを特徴とする請求項４または５に記載の電子透かし埋め込み装置。

【請求項７】

前記デジタルコンテンツの複製物に電子透かしとして埋め込むために使用可能とする前記識別情報の範囲を、前記シンボル列を割り当て可能な識別情報の範囲よりも狭い範囲に制限したことを特徴とする請求項１ないし６のいずれか１項に記載の識別情報復号装置。

【請求項８】

前記識別情報は、前記デジタルコンテンツの複製物を提供するユーザに固有の情報であることを特徴とする請求項１ないし７のいずれか１項に記載の電子透かし埋め込み装置。

【請求項９】

互いに異なる識別情報を電子透かしとして埋め込まれた複数のデジタルコンテンツの複製物をもとにして結託攻撃によって作出された不正のデジタルコンテンツの複製物を対象として、結託攻撃に用いられたデジタルコンテンツの複製物に埋め込まれていた識別情報を特定するための電子透かし解析装置であって、

前記デジタルコンテンツの複製物から、序列を持った複数の埋め込み符号をそれぞれ抽出する第１の抽出手段と、

抽出された前記複数の埋め込み符号にそれぞれ対応するシンボルを求め、求められた複数のシンボル列を、対応する埋め込み符号の序列に従って並べてシンボル列を求める第２の抽出手段と、

前記結託攻撃に用いられたデジタルコンテンツの複製物から抽出された前記シンボル列及び各々の正当な識別情報に対してそれぞれ一意に割り当てられるシンボル列に基づいて、前記結託攻撃に用いられたデジタルコンテンツの複製物に埋め込まれていた識別情報を特定する追跡手段とを備えたことを特徴とする電子透かし解析装置。

【請求項１０】

結託攻撃を受ける前の前記デジタルコンテンツの複製物に電子透かしとして埋め込む前記識別情報には、当該識別情報に一意に対応する、序列を持った複数のシンボルの並びからなるシンボル列が割り当てられており、

前記デジタルコンテンツの複製物には、前記シンボル列を構成する個々の序列のシンボルごとにそれぞれ対応する埋め込み符号が電子透かしとして埋め込まれていることを特徴とする請求項９に記載の電子透かし解析装置。

【請求項１１】

前記第１の抽出手段は、個々の前記序列ごとに、前記結託攻撃において最も多く使用されたと評価される埋め込み符号を抽出することを特徴とする特徴とする請求項９または１０に記載の電子透かし解析装置。

【請求項１２】

前記埋め込み符号は、前記シンボル列の個々の序列において、同一の序列に属する互いに異なるシンボルに対応する埋め込み符号同士が、相互相関の無い又は小さい乱数列になるように、生成されたものであり、

前記第１の抽出手段は、個々の前記序列ごとに、当該序列で使用される複数の埋め込み符号の各々について、前記デジタルコンテンツの複製物との相関を取り、相関値が最大であった埋め込み符号を抽出することを特徴とする請求項９ないし１１のいずれか１項に記載の電子透かし解析装置。

【請求項１３】

前記埋め込み符号は、前記シンボル列の異なる序列に属するシンボルに対応す

る埋め込み符号同士についても、相互相関の無い又は小さい乱数列になるように、生成されたものであることを特徴とする請求項１２に記載の電子透かし解析装置。

【請求項１４】

前記第２の抽出手段は、全ての識別情報について、当該識別情報に一意に対応するシンボル列と、前記対象となったデジタルコンテンツの複製物から求められた抽出シンボル列とを比較した結果に基づいて、前記結託攻撃に用いられたデジタルコンテンツの複製物に埋め込まれていた識別情報を特定することを特徴とする請求項９ないし１３のいずれか１項に記載の電子透かし解析装置。

【請求項１５】

前記第２の抽出手段は、全ての識別情報について、当該識別情報に一意に対応するシンボル列と、前記対象となったデジタルコンテンツの複製物から求められた抽出シンボル列とを、各序列ごとにそれぞれ比較し、予め定められた個数以上の序列におけるシンボルの一致が得られた場合に、当該識別情報を、前記結託攻撃に用いられたデジタルコンテンツの複製物に埋め込まれていた識別情報として特定することを特徴とする請求項１４に記載の電子透かし解析装置。

【請求項１６】

前記識別情報は、整数値であり、且つ、前記シンボル列の各序列ｉごとに対応して特定の整数値Ｎ（ｉ）が予め定められており（ここで、Ｎ（０）≦Ｎ（１）≦…≦Ｎ（Ｍ）とする）、且つ、前記第１の生成手段は、前記識別情報の値に基づき、前記シンボル列の個々の序列ｉに対応するシンボルＳ（ｉ）を、０からＮ（ｉ）－１の範囲で選択し、これによって得られた個々の序列ｉに対応するシンボルＳ（ｉ）を当該序列に従って並べたものを、生成すべきシンボル列とするものである場合に、

前記予め定められた個数を、ｋ＋１とする（ただし、ｋは、Ｎ（０），…，Ｎ（ｋ）の積が前記識別情報の総数以上となるような値であり、１は［１－Π　１／Ｎ（ｉ）］^{S}≧１－ε_2（ただし、Πをとるｉの範囲は、ｉ＝０～（１－１）又はｉ＝ｋ～（ｋ＋１－１）であり、Ｓは、$_{M}C_{k+1}$であり、ε_2（ただし、０＜ε_2＜１）は、前記結託攻撃に用いられたデジタルコンテンツの複製物に埋め込

まれていた識別情報として誤った識別情報を特定してしまう追跡誤り率である）により与えられる値である）ことを特徴とする請求項１５に記載の電子透かし解析装置。

【請求項１７】

前記識別情報は、整数値であり、且つ、前記シンボル列の各序列ｉごとに対応して特定の整数値Ｎ（ｉ）が予め定められており（ここで、ｑ＝Ｎ（０）＝Ｎ（１）＝…＝Ｎ（Ｍ）とする）、且つ、前記第１の生成手段は、前記識別情報の値に基づき、前記シンボル列の個々の序列ｉに対応するシンボルＳ（ｉ）を、０からＮ（ｉ）－１の範囲で選択し、これによって得られた個々の序列ｉに対応するシンボルＳ（ｉ）を当該序列に従って並べたものを、生成すべきシンボル列とするものである場合に、

前記予め定められた個数を、ｋ＋１とする（ただし、ｋは、Ｎ（０），…，Ｎ（ｋ）の積が前記識別情報の総数以上となるような値であり、ｌは［１－１／ｑ^{l}］^{S}≧１－ε（ただし、Ｓは、$_{M}C_{k+l}$であり、ε（ただし、０＜ε＜１）は、前記結託攻撃に用いられたデジタルコンテンツの複製物に埋め込まれていた識別情報として誤った識別情報を特定してしまう追跡誤り率である）により与えられる値である）ことを特徴とする請求項１５に記載の電子透かし解析装置。

【請求項１８】

前記第２の抽出手段は、予め定められた最大結託数以下の結託数による任意の識別情報の組合せからなる結託グループのうち、前記対象となったデジタルコンテンツの複製物から抽出された前記シンボル列を作出可能な１又は複数の結託グループを特定し、該特定した１又は複数の結託グループをそれぞれ構成する識別情報の組合せに基づいて、前記結託攻撃に用いられたデジタルコンテンツの複製物に埋め込まれていた識別情報として特定することを特徴とする請求項９ないし１３のいずれか１項に記載の電子透かし解析装置。

【請求項１９】

前記第２の抽出手段は、前記対象となったデジタルコンテンツの複製物から抽出された前記シンボル列を作出可能な結託グループが１つのみ特定された場合には、該特定された結託グループを構成する識別情報を全て、前記結託攻撃に用い

られたデジタルコンテンツの複製物に埋め込まれていた識別情報として特定することを特徴とする請求項１８に記載の電子透かし解析装置。

【請求項２０】

前記第２の抽出手段は、前記対象となったデジタルコンテンツの複製物から抽出された前記シンボル列を作出可能な結託グループが複数特定された場合には、該特定された結託グループの全てに共通に含まれる識別情報のみを、前記結託攻撃に用いられたデジタルコンテンツの複製物に埋め込まれていた識別情報として特定することを特徴とする請求項１８または１９に記載の電子透かし解析装置。

【請求項２１】

前記デジタルコンテンツの複製物に電子透かしとして埋め込むために使用可能とする前記識別情報の範囲を、前記シンボル列を割り当て可能な識別情報の範囲よりも狭い範囲に制限したことを特徴とする請求項９ないし２０のいずれか１項に記載の電子透かし解析装置。

【請求項２２】

前記識別情報は、前記デジタルコンテンツの複製物を提供するユーザに固有の情報であることを特徴とする請求項９ないし２１のいずれか１項に記載の電子透かし解析装置。

【請求項２３】

デジタルコンテンツの複製物に電子透かしとして埋め込むべき識別情報に一意に対応する、序列を持った複数のシンボルの並びからなるシンボル列を生成し、

生成された前記シンボル列を構成する個々の序列のシンボルごとに、対応する埋め込み符号をそれぞれ生成し、

生成された前記個々の序列のシンボルにそれぞれ対応する埋め込み符号を、前記デジタルコンテンツの複製物に電子透かしとして埋め込むことを特徴とする電子透かし埋め込み方法。

【請求項２４】

互いに異なる識別情報を電子透かしとして埋め込まれた複数のデジタルコンテンツの複製物をもとにして結託攻撃によって作出された不正のデジタルコンテンツの複製物を対象として、結託攻撃に用いられたデジタルコンテンツの複製物に

埋め込まれていた識別情報を特定するための電子透かし解析方法あって、

前記デジタルコンテンツの複製物から、序列を持った複数の埋め込み符号をそれぞれ抽出し、

抽出された前記複数の埋め込み符号にそれぞれ対応するシンボルを求め、求められた複数のシンボル列を、対応する埋め込み符号の序列に従って並べてシンボル列を求め、

前記結託攻撃に用いられたデジタルコンテンツの複製物から抽出された前記シンボル列及び各々の正当な識別情報に対してそれぞれ一意に割り当てられるシンボル列に基づいて、前記結託攻撃に用いられたデジタルコンテンツの複製物に埋め込まれていた識別情報を特定することを特徴とする電子透かし解析方法。

【請求項２５】

コンピュータを電子透かし埋め込み装置として機能させるためのプログラムであって、

デジタルコンテンツの複製物に電子透かしとして埋め込むべき識別情報に一意に対応する、序列を持った複数のシンボルの並びからなるシンボル列を生成する機能と、

生成された前記シンボル列を構成する個々の序列のシンボルごとに、対応する埋め込み符号をそれぞれ生成する機能と、

生成された前記個々の序列のシンボルにそれぞれ対応する埋め込み符号を、前記デジタルコンテンツの複製物に電子透かしとして埋め込む機能とをコンピュータに実現させるためのプログラム。

【請求項２６】

互いに異なる識別情報を電子透かしとして埋め込まれた複数のデジタルコンテンツの複製物をもとにして結託攻撃によって作出された不正のデジタルコンテンツの複製物を対象として、結託攻撃に用いられたデジタルコンテンツの複製物に埋め込まれていた識別情報を特定するための電子透かし解析装置として、コンピュータを機能させるためのプログラムであって、

前記デジタルコンテンツの複製物から、序列を持った複数の埋め込み符号をそれぞれ抽出する機能と、

抽出された前記複数の埋め込み符号にそれぞれ対応するシンボルを求め、求められた複数のシンボル列を、対応する埋め込み符号の序列に従って並べてシンボル列を求める機能と、

前記結託攻撃に用いられたデジタルコンテンツの複製物から抽出された前記シンボル列及び各々の正当な識別情報に対してそれぞれ一意に割り当てられるシンボル列に基づいて、前記結託攻撃に用いられたデジタルコンテンツの複製物に埋め込まれていた識別情報を特定する機能機能とをコンピュータに実現させるためのプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、識別情報に対応する埋め込み符号を生成しコンテンツの複製物に埋め込む電子透かし埋め込み装置及び電子透かし埋め込み方法、結託攻撃に用いられたコンテンツの複製物に埋め込まれていた埋め込み符号に対応する識別情報を求める電子透かし解析装置及び方法並びにプログラムに関する。

【０００２】

【従来の技術】

デジタルコンテンツ（例えば、静止画、動画、音声、音楽等）は、多数のデジタルデータで構成された構造を持つ。そして、その構造の中には、データを変更しても、当該デジタルコンテンツの作品の同一性あるいは経済的価値を保持できる部分がある。そのような許容された範囲内のデータを適宜変更するによって、デジタルコンテンツに、種々の情報を埋め込むことができる。このような技術は、電子透かしとして、良く知られている。

【０００３】

電子透かし技術によって、デジタルコンテンツに、様々な透かし情報（例えば、コンテンツの著作権者やユーザを識別する情報、著作権者の権利情報、コンテンツの利用条件、その利用時に必要な秘密情報、コピー制御情報等、あるいはそれらを組み合わせたものなど）を、様々な目的（例えば、利用制御、コピー制御を含む著作権保護、二次利用の促進等）で埋め込み、検出・利用することができ

る。

【０００４】

ここでは、例えば同一のデジタルコンテンツを多数のユーザを対象として配給するときに適用される技術として、デジタルコンテンツの複製物に、当該複製物を個々に識別するための情報（例えば、ユーザＩＤに一意に対応する透かし情報）を埋め込む場合を考える。

【０００５】

デジタルコンテンツの複製物に固有の識別情報（に対応する符号）を埋め込む手法は、そのデジタルコンテンツの複製物が更に複製されて海賊版として出回ったときに、該海賊版から識別情報を検出することによって流出元ユーザを特定することができることから、デジタルコンテンツの違法コピーに対する事前の抑制として機能するとともに、著作権侵害が発生したときの事後の救済にも役立つことになる。

【０００６】

また、あるユーザがデジタルコンテンツの複製物に埋め込まれた識別情報を無効にするためには、ユーザにはどの部分が識別情報（に対応する符号）を構成するビットであるか分からないので、当該デジタルコンテンツの複製物に相当の改変を加える必要があり、そうすると、当該デジタルコンテンツの経済的価値を損なってしまうので、違法コピーの動機付けを奪うことができる。

【０００７】

このような状況において違法コピーを可能ならしめる方法として出現したのが、「結託攻撃（ｃｏｌｌｕｓｉｏｎ　ａｔｔａｃｋ）」である。

【０００８】

結託攻撃は、異なる複製物には異なる識別情報が埋めこまれていることを利用するものである。例えば、複数人で複製物を持ち寄って、それらをビット単位で比較することによって、デジタルデータの値が異なる部分を見つけ出し、その部分を改ざん（例えば、多数決、少数決、ランダマイズ等）することによって、識別情報を改ざん、消失させる。あるいは、具体的な比較操作は行わず、コンテンツ間で画素値を平均化するなどの操作を行って、識別情報を改ざん、消失させる

【０００９】

例えば簡単な例で示すと、Ａ氏、Ｂ氏、Ｃ氏の複製物にそれぞれ、

Ａ　：　１０…００…

Ｂ　：　００…１１…

Ｃ　：　１１…０１…

という識別情報（実際には、これに対応する符号）が埋め込まれていた場合に、例えば、多数決あるいは平均化等によって、

１０…０１…

というように、Ａ氏、Ｂ氏、Ｃ氏のいずれとも異なる識別情報が検出されるようなコンテンツを出現させることができてしまう。

【００１０】

そこで、結託攻撃に対する耐性、すなわち結託攻撃を受けても結託者の全部または一部を特定できるような性質を持つ符号（結託耐性符号と呼ばれる）を電子透かしとして埋め込む方法および該結託耐性符号に基づく追跡アルゴリズム（ｔｒａｃｉｎｇ　ａｌｇｏｒｉｔｈｍ；結託攻撃に用いられたコンテンツに埋め込まれた識別番号を特定し、結託者のユーザＩＤを特定するためのアルゴリズム）が種々提案されている。例えば、ｃ－ｓｅｃｕｒｅ　符号(D. Boneh and J. Shaw, “Collusion-Secure Fingerprinting for Digital Data,” CRYPTO’95, 180-189, 1995.)やｃ－ｓｅｃｕｒｅ　ＣＲＴ　符号(Hirofumi Muratani, “A Collusion-Secure Fingerprinting Code Reduced by Chinese Remaindering and its Random-Error Resilience” ,Information Hiding Workshop 2001, 301-315, 2001.や、特開２００１－２８５６２３号公報)がその例である。

【００１１】

ここで、ｃ－ｓｅｃｕｒｅ　ＣＲＴ符号について簡単に説明する。

【００１２】

ｃ－ｓｅｃｕｒｅ　ＣＲＴ符号は、Ｍ個の成分符号を連接してなる連接符号の構造を持つ。例えば、第１番目の成分符号Ｗ（ｉ）は、０のみからなるか、１のみからなるか、または０と１が混在する（ただし、０と１の境界はただ１つであ

る）、所定長のビット列であって、識別情報ｕを法ｐ（ｉ）で除したときの剰余によって、成分符号Ｗ（ｉ）に含まれる０のビット数及び１のビット数、すなわち、成分符号Ｗ（ｉ）を構成するビット列における０の系列と１の系列との境界位置が決定されるような符号である。

【００１３】

例えば、Ｍ＝３とし、ｐ（１）＝３，ｐ（２）＝５，ｐ（３）＝７とし、成分符号Ｗ（ｉ）としてΓ_0(ｎ，ｄ)符号（１または０のみからなる連続したビットを一つの単位Ｂ（ｊ）とし、Ｂ（０）～Ｂ（ｎ－２）を連結したもの；ただし、Ｂ（０）～Ｂ（ｎ－２）は、すべてが０のみからなるか、すべてが１のみからなるか、またはＢ（０）～Ｂ（ｍ－１）までは０のみからなり且つＢ（ｍ）～Ｂ（ｎ－２）までは１のみからなるもの）を用いるものとし（ｄ＝３とする）、識別情報＝ユーザＩＤとすると、

例えば、ユーザＩＤ＝２に対応する符号は、

000000　000000111111　000000111111111111

となり、ユーザＩＤ＝３に対応する符号は、

111111　000000000111　000000000111111111

となる。

【００１４】

この場合に、ユーザＩＤ＝２のユーザとユーザＩＤ＝３の２人のユーザが持ちよったコンテンツを比較すると、上記３６ビットのうち、左から１～６番目、１３～１５番目、２５～２７番目が相違していることがわかる。そこで、それらが識別情報に対応する符号の一部と分かるため、１～６番目、１３～１５番目、２５～２７番目のうちの一部に改ざんが施され、例えば、

010101　000000010111　000000101111111111

というように、ユーザＩＤ＝２とユーザＩＤ＝３のいずれとも異なる識別情報が検出されるようなコンテンツが作出される。

【００１５】

ところが、正当なユーザＩＤに対応する符号は、予め定められたブロックのサイズｄ（上記の例の場合、３）ビット未満の数の１や０が孤立して存在する部分

は存在しないが、これに対して、上記のように結託攻撃を受けたコンテンツから検出される符号は、持ち寄ったコンテンツ同士で相違する符号部分については、０と１が混在しており、すなわち、ｄ（上記の例の場合、３）ビット未満の数の１や０が孤立して存在する部分が存在することが分かる。

【００１６】

そこで、追跡アルゴリズムでは、検出された符号の各々の成分符号を調べ、予め定められたｄ（上記の例の場合、３）ビット未満の数の１や０が孤立して存在する成分符号が検出された場合に、結託攻撃がなされたものと判断することができる。

【００１７】

ところで、ｃ－ｓｅｃｕｒｅ　ＣＲＴ符号では、追跡対象コンテンツから検出された符号の第ｉ番目の成分符号Ｗ（ｉ）を、左端のビットからみていったときにはじめて出現する、０のみからなる要素と１を含む要素との境界の位置（を表す整数値）を最小剰余とし、右端のビットからみていったときにはじめて出現する、１のみからなる要素と０を含む要素との境界の位置（を表す整数値）を最大剰余とすると、最大剰余及び最小剰余（＝剰余対）は、いずれかの結託者の識別情報ｕに対する剰余すなわちｕ　ｍｏｄ　ｐ（ｉ）と等しくなるという性質がある。なお、第ｉ番目の成分符号Ｗ（ｉ）が０のみからなる場合には、最小剰余＝最大剰余＝ｐ（ｉ）－１、第ｉ番目の成分符号Ｗ（ｉ）が１のみからなる場合には、最小剰余＝最大剰余＝０、０のみからなる要素と１を含む要素との境界がない場合には、最小剰余＝０、１のみからなる要素と０を含む要素との境界がない場合には、最大剰余＝ｐ（ｉ）－１とする。

【００１８】

したがって、追跡対象コンテンツから検出されたｃ－ｓｅｃｕｒｅ　ＣＲＴ符号の各成分部号から求めた剰余対を解析することによって、結託攻撃に使用された複製物に埋め込まれていたであろう識別情報の一部又は全部を求めることができるようになる。

【００１９】

上記の例の場合、

010101　000000010111　000000101111111111

という符号から、

結託者の識別情報として、ユーザＩＤ＝２とユーザＩＤ＝３を特定することができる。

【００２０】

このｃ－ｓｅｃｕｒｅ　ＣＲＴ符号は、次のようなマーキング仮定に基づいている。すなわち、結託攻撃に参加している結託者の中に、ある成分符号中のあるビットに対して異なる値を持つ者がいる場合に、結託攻撃の結果、生成される成分符号におけるそのビットがいずれの値をとるかは、確率的に決まる。よって、ブロックのサイズｄがある程度大きくなると、正しく最小剰余及び最大剰余を検出することができる。

【００２１】

【発明が解決しようとする課題】

ｃ－ｓｅｃｕｒｅ　ＣＲＴ符号において、具体的場合においては、追跡対象コンテンツから上記の最小剰余及び最大剰余を正しく検出できないケースが存在し得る。

【００２２】

例えば、１００人での結託攻撃を考えた場合、成分符号中あるブロックにおいて、９９人にはビット列０が残りの一人にはビット列１が割り当てられていたとする。マーキング仮定では、０でも１でもないビット列がある確率で検出されることを期待している。ところが、電子透かしでは、ある測定量が所定のしきい値を越えるか否かでビット値の判定を行う場合が多く、結託攻撃がコンテンツの平均操作の場合、結託攻撃後の測定量は攻撃前の測定量の平均となると期待され、９９対１の平均では、９９人側の測定量の影響が大きく、ビット列は、９９人側の値０として検出される確率が大きい。このブロックが最小剰余及び最大剰余を検出する境界のブロックならば、正しく最小剰余及び最大剰余を検出できないことになる。なお、これを符号感度の問題と呼ぶ。

【００２３】

本発明は、上記事情を考慮してなされたもので、結託攻撃に用いられたコンテ

ンツの複製物に埋め込まれていたであろう識別情報を、より感度の高い符号によって推定可能とした電子透かし埋め込み装置、電子透かし解析装置、電子透かし埋め込み方法、電子透かし解析方法及びプログラムを提供することを目的とする。

【００２４】

【課題を解決するための手段】

本発明に係る電子透かし埋め込み装置によれば、デジタルコンテンツの複製物に電子透かしとして埋め込むべき識別情報に一意に対応する、序列を持った複数のシンボルの並びからなるシンボル列を生成する第１の生成手段と、生成された前記シンボル列を構成する個々の序列のシンボルごとに、対応する埋め込み符号をそれぞれ生成する第２の生成手段と、生成された前記個々の序列のシンボルにそれぞれ対応する埋め込み符号を、前記デジタルコンテンツの複製物に電子透かしとして埋め込む符号埋め込み手段とを備えたことを特徴とする。

【００２５】

また、本発明は、互いに異なる識別情報を電子透かしとして埋め込まれた複数のデジタルコンテンツの複製物をもとにして結託攻撃によって作出された不正のデジタルコンテンツの複製物を対象として、結託攻撃に用いられたデジタルコンテンツの複製物に埋め込まれていた識別情報を特定するための電子透かし解析装置であって、前記デジタルコンテンツの複製物から、序列を持った複数の埋め込み符号をそれぞれ抽出する第１の抽出手段と、抽出された前記複数の埋め込み符号にそれぞれ対応するシンボルを求め、求められた複数のシンボル列を、対応する埋め込み符号の序列に従って並べてシンボル列を求める第２の抽出手段と、前記結託攻撃に用いられたデジタルコンテンツの複製物から抽出された前記シンボル列及び各々の正当な識別情報に対してそれぞれ一意に割り当てられるシンボル列に基づいて、前記結託攻撃に用いられたデジタルコンテンツの複製物に埋め込まれていた識別情報を特定する追跡手段とを備えたことを特徴とする。

【００２６】

また、本発明は、デジタルコンテンツの複製物に電子透かしとして埋め込むべき識別情報に一意に対応する、序列を持った複数のシンボルの並びからなるシン

ボル列を生成し、生成された前記シンボル列を構成する個々の序列のシンボルごとに、対応する埋め込み符号をそれぞれ生成し、生成された前記個々の序列のシンボルにそれぞれ対応する埋め込み符号を、前記デジタルコンテンツの複製物に電子透かしとして埋め込むことを特徴とする。

【００２７】

また、本発明は、互いに異なる識別情報を電子透かしとして埋め込まれた複数のデジタルコンテンツの複製物をもとにして結託攻撃によって作出された不正のデジタルコンテンツの複製物を対象として、結託攻撃に用いられたデジタルコンテンツの複製物に埋め込まれていた識別情報を特定するための電子透かし解析方法あって、前記デジタルコンテンツの複製物から、序列を持った複数の埋め込み符号をそれぞれ抽出し、抽出された前記複数の埋め込み符号にそれぞれ対応するシンボルを求め、求められた複数のシンボル列を、対応する埋め込み符号の序列に従って並べてシンボル列を求め、前記結託攻撃に用いられたデジタルコンテンツの複製物から抽出された前記シンボル列及び各々の正当な識別情報に対してそれぞれ一意に割り当てられるシンボル列に基づいて、前記結託攻撃に用いられたデジタルコンテンツの複製物に埋め込まれていた識別情報を特定することを特徴とする。

【００２８】

また、本発明は、コンピュータを電子透かし埋め込み装置として機能させるためのプログラムであって、デジタルコンテンツの複製物に電子透かしとして埋め込むべき識別情報に一意に対応する、序列を持った複数のシンボルの並びからなるシンボル列を生成する機能と、生成された前記シンボル列を構成する個々の序列のシンボルごとに、対応する埋め込み符号をそれぞれ生成する機能と、生成された前記個々の序列のシンボルにそれぞれ対応する埋め込み符号を、前記デジタルコンテンツの複製物に電子透かしとして埋め込む機能とをコンピュータに実現させるためのプログラムである。

【００２９】

また、本発明は、互いに異なる識別情報を電子透かしとして埋め込まれた複数のデジタルコンテンツの複製物をもとにして結託攻撃によって作出された不正の

デジタルコンテンツの複製物を対象として、結託攻撃に用いられたデジタルコンテンツの複製物に埋め込まれていた識別情報を特定するための電子透かし解析装置として、コンピュータを機能させるためのプログラムであって、前記デジタルコンテンツの複製物から、序列を持った複数の埋め込み符号をそれぞれ抽出する機能と、抽出された前記複数の埋め込み符号にそれぞれ対応するシンボルを求め、求められた複数のシンボル列を、対応する埋め込み符号の序列に従って並べてシンボル列を求める機能と、前記結託攻撃に用いられたデジタルコンテンツの複製物から抽出された前記シンボル列及び各々の正当な識別情報に対してそれぞれ一意に割り当てられるシンボル列に基づいて、前記結託攻撃に用いられたデジタルコンテンツの複製物に埋め込まれていた識別情報を特定する機能機能とをコンピュータに実現させるためのプログラムである。

【００３０】

なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。

また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムとしても成立し、該プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【００３１】

本発明によれば、結託攻撃に用いられたコンテンツの複製物に埋め込まれていたであろう識別情報を、より感度の高い符号によって推定することができるようになる。また、符号長の短縮にも有効である。

【００３２】

【発明の実施の形態】

以下、図面を参照しながら発明の実施の形態を説明する。

【００３３】

同一のデジタルコンテンツの複製物（例えば、静止画、動画、音声、音楽等）の各々に対して、当該複製物ごとに異なる識別情報を透かし情報として埋め込み

、追跡する場合について説明する。以下では、識別情報として、当該複製物に対応するユーザすなわち当該複製物を利用することになるユーザ（例えば、当該複製物を記録媒体又は通信媒体を媒介として譲渡し若しくは貸し渡し又は提供する対象となるユーザ）のユーザ識別子（ユーザＩＤ）を用いる場合を主として説明するが、ユーザＩＤに対して所定の変換を施したものを識別情報としてもよいし、ユーザＩＤ以外の情報又はユーザＩＤ以外の情報を変換した情報を識別情報としてもよい。なお、ユーザＩＤには、利用の日時や利用場所等の情報を含めても良い。

【００３４】

もちろん、デジタルコンテンツの複製物に対して、さらに、その他の様々な透かし情報（例えば、コンテンツの著作権者に関する情報、著作権等の権利に関する情報、コンテンツの利用条件に関する情報、その利用時に必要な秘密情報、コピー制御情報等、あるいはそれらを組み合わせたものなど）が様々な目的（例えば、利用制御、コピー制御を含む著作権保護、二次利用の促進等）で埋め込まれ、検出されてもよいが、その他の透かし情報を利用する場合における当該その他の透かし情報に関係する部分の構成は任意である。

【００３５】

以下で示す構成図は、装置の機能ブロック図としても成立し、また、ソフトウェア（プログラム）の機能モジュール図あるいは手順図としても成立するものである。

【００３６】

図１に、本発明の実施の形態に係る電子透かし埋込装置と電子透かし解析装置が適用されるシステムの概念図を示す。

【００３７】

電子透かし埋込装置１と電子透かし解析装置２は、例えば、コンテンツ提供側に備えられ、管理される。

また、例えば、電子透かし埋込装置１は、ユーザ側に備えられ（例えば、コンテンツを利用するためのユーザ・システム（例えば、計算機システムや専用機器等に接続されあるいは組み込まれるなど）、電子透かし解析装置２は、コンテン

ツ提供側に備えられるようにしてもよい。

デジタルコンテンツの複製物への透かし情報の埋め込みは、前者の場合、該複製物がユーザへ渡されるのに先だって行われ、後者の場合、該複製物がユーザの利用に供されるのに先だって行われることになる。

【００３８】

電子透かし埋込装置１においてデジタルコンテンツに所望の透かしデータを埋め込む方法や、電子透かし解析装置２においてデジタルコンテンツから該透かしデータ自体を取り出す方法は、どのような方法であってもよい（例えば、“松井甲子雄著、「電子透かしの基礎」、森北出版、１９９８年”等参照）。

電子透かし埋込装置１は、ソフトウェア（プログラム）としてもハードウェアとしても実現可能である。同様に、電子透かし解析装置２は、ソフトウェア（プログラム）としてもハードウェアとしても実現可能である。また、電子透かし埋込装置１および電子透かし解析装置２をコンテンツ提供側で用いる場合には、それらを一体化して実現することも可能である。

【００３９】

図２に、電子透かし埋込装置１の構成例を示す。

【００４０】

図２に示されるように、電子透かし埋込装置１は、埋め込むべき識別情報（例えば、ユーザＩＤ）に対応するシンボル列を生成するシンボル列生成部１１と、シンボル列の各シンボルにそれぞれ対応する埋め込み符号（例えば、乱数列）を生成する埋め込み符号生成部１２と、生成された埋め込み符号を対象コンテンツに埋め込む符号埋込部１３とから構成される。

【００４１】

電子透かし埋込装置１は、埋込対象コンテンツと、これに埋め込むべき識別情報（例えば、当該コンテンツを提供すべき対象ユーザのユーザＩＤ）とが与えられると、該識別情報に対応するシンボル列を生成し、生成されたシンボル列の各シンボルにそれぞれ対応する埋め込み符号を生成し、各埋め込み符号を対象コンテンツに埋め込んで、これを該識別情報に対応する複製物（例えば、該ユーザＩＤのユーザ向けの複製物）として出力する。他の透かし情報を利用する場合には

、必要に応じて他の透かし情報も埋め込まれる。

【００４２】

なお、例えば、識別情報≠ユーザＩＤであって、かつ、ユーザＩＤが与えられるような場合には、与えられたユーザＩＤを識別情報に変換する、などの前処理を行う。

【００４３】

電子透かし埋込装置１により得られた当該識別情報に対応するコンテンツの複製物は、記憶媒体や通信媒体などを媒介とした流通経路３を経てそれぞれ流通する。複数の複製物を用いた結託攻撃は、この流通経路３にて行われる。

【００４４】

ここでは、結託攻撃としては、例えば、複数の複製物の単純平均操作（結託させる全コンテンツの重みを同一にして平均する）あるいは重み付け平均操作（結託させる全コンテンツの重みが全て同一ではないようにして平均する）などを想定している。

【００４５】

図３に、電子透かし解析装置２の構成例を示す。

【００４６】

図３に示されるように、電子透かし解析装置２は、埋め込み符号抽出部２１と、シンボル列抽出部２２と、追跡部２３とを備えている。

【００４７】

埋め込み符号抽出部２１は、追跡対象コンテンツから、抽出すべきシンボル列の各シンボルにそれぞれ対応する埋め込み符号を抽出する。

【００４８】

シンボル列抽出部２２は、抽出された各抽出埋め込み符号からそれぞれ対応する抽出シンボルを求め、それら各抽出シンボルからなるシンボル列を出力する。

【００４９】

追跡部２３は、抽出シンボル列に対して、所定の追跡アルゴリズムを適用することによって、結託攻撃がなかったこと、または結託攻撃に用いられた複数の複製物にそれぞれ埋め込まれていた全識別情報（例えば、ユーザＩＤ）のうちの全

部又は一部を、特定（あるいは推測）しようとする。

【００５０】

なお、例えば、識別情報≠ユーザＩＤであって、ユーザＩＤを求める必要があるような場合には、特定された識別情報を、さらに、ユーザＩＤに変換する、などの後処理を行う。

【００５１】

なお、追跡アルゴリズム及びその前提となるシンボル列生成方法には種々のものがあり、例えば、一定の誤検出を許容して結託者の識別情報を求める確率論的方法や、誤検出なしに結託者の識別情報を求める決定論的方法などがある。

【００５２】

以下、本実施形態についてより詳細に説明する。

【００５３】

なお、以下では、識別情報＝ユーザＩＤの場合を具体例にとって説明する（したがって、以下において、識別情報＝ユーザＩＤとして説明している場合には、ユーザＩＤは一般的には識別情報のことを意味している）。

【００５４】

また、以下では、各識別情報には、当該識別情報に固有となるシンボル列を割り当てるものとして説明する。なお、あるシンボル列に複数の識別情報が対応することを許す方法も可能である。

【００５５】

まず、電子透かし埋込装置１について説明する。

【００５６】

図４に、概略的な手順の一例を示す。

【００５７】

シンボル列生成部１１は、まず、対象複製物に埋め込むべき識別情報（本具体例では、ユーザＩＤ）に対応する、Ｍ（Ｍは複数）個のシンボルの並びからなるシンボル列｛Ｓ（１），Ｓ（２），…，Ｓ（Ｍ）｝を求める（ステップＳ１）。

【００５８】

ここで、Ｓ（１）は、該識別情報に割り当てられたシンボル列すなわちシンボ

ルの並びにおける第１番目の序列に位置するシンボルすなわち第１シンボル（の値）を表し、Ｓ（２）～Ｓ（Ｍ）についても同様である。

【００５９】

なお、該シンボル列は、各識別情報に対応して予め求めて記憶しておく方法と、必要時に生成する方法とがある。

【００６０】

識別情報に対してシンボル列は一意に対応するので、ある正しい識別情報に対応するシンボル列｛Ｓ（１），Ｓ（２），…，Ｓ（Ｍ）｝が与えられると、該シンボル列に対応する識別情報が一意に特定されることになる。なお、結託攻撃を施された複製物から抽出した抽出シンボル列から、その結託攻撃に使用された識別情報を求めるのが、追跡アルゴリズムである。

【００６１】

ここで、シンボルは、互いに区別できるものであれば、どのようなものでもよい。例えば、１つのシンボルとして、整数（または整数列）を用いてもよいし、アルファベット（またはアルファベット列）を用いてもよいし、英数字（または英数字列）を用いてもよいし、他のものでもよい。

【００６２】

また、第１シンボルＳ（１）の取り得る値（すなわち第１シンボルＳ（１）の元）と、第２シンボルＳ（２）の取り得る値と、…、第ＭシンボルＳ（Ｍ）の取り得る値とは、互いに異なるものであってもよいし、全て同一でもよい。例えば、シンボルとして整数を用いる場合に、第１シンボルＳ（１）は０～２のいずれかを取るものであり、第２シンボルＳ（２）は０～４のいずれかを取るものであり、第３シンボルＳ（３）は０～６のいずれかを取るものであり、…というように、互いに取り得る値の範囲の異なるものであってもよいし、第１シンボルＳ（１）と第２シンボルＳ（２）は１～３のいずれかを取るものであり、第３シンボルＳ（３）は０～６のいずれかを取るものであり、…というように、一部は同じで一部は異なるようなものであってもよいし、Ｓ（１），Ｓ（２），…，Ｓ（Ｍ）の全てが０～１４のいずれかを取るものというように、全て同一でもよい。また、第１シンボルＳ（１）には整数を用い、第２シンボルＳ（２）にはアルファ

ベットを用い…、というような構成も可能である。

【００６３】

以下では、具体例を用いて説明する場合には、シンボルに整数を用いる例を中心に説明する。なお、例えば、まず整数を求め、求められた整数を対応するアルファベットに変換してそれをシンボルとして用いるものとする場合には、以下の説明において整数とアルファベットとの間の変換処理を追加すればよい。

【００６４】

さて、与えられた識別情報から、それに一意に対応するシンボル列｛Ｓ（１），Ｓ（２），…，Ｓ（Ｍ）｝を求める方法には、種々のバリエーションがある。

【００６５】

例えば、第ｉのシンボルＳ（ｉ）が、０～Ｎ（ｉ）－１の範囲内の整数値のいずれかを取るようにしてもよい。ここで、Ｎ（１）、Ｎ（２）、…、Ｎ（Ｍ）は、例えば、予め定められた相互に異なる正整数である（互いに素の関係にある整数とするのが望ましい）。なお、Ｎ（１）＜Ｎ（２）＜…＜Ｎ（Ｍ）としてもよいし、また、Ｎ（１）＝Ｎ（２）＝…＝Ｎ（Ｍ）とする方法もあるし、他の方法もある。

【００６６】

識別情報に対応するシンボル列の第ｉシンボルＳ（ｉ）（ｉ＝１～Ｍ）の各々には、０～Ｎ（ｉ）－１の範囲でランダムに値を割り当てる方法と、０～Ｎ（ｉ）－１の範囲で一定の規則に従って値を割り当てる方法とがある。また、いずれの場合においても、各識別情報には、互いにＳ（１）、Ｓ（２）、…、Ｓ（Ｍ）のうちの少なくとも一つが相違するように、Ｍ個のシンボルの組を排他的に割り当てるものとする。

【００６７】

各識別情報に固有のシンボル列を割り当てるシンボル列生成方法には、例えば、識別情報の値として、０～Ｎ（１）×Ｎ（２）×…×Ｎ（Ｍ）－１の範囲の整数の全部または一部を使用するものとし、対象となる識別情報ＵをＮ（ｉ）で割ったときの剰余Ｕ　ｍｏｄ　Ｎ（ｉ）を、該識別情報に対応するＳ（ｉ）の値とする方法がある。この場合、これらＭ個の数Ｎ（１）、Ｎ（２）、…、Ｎ（Ｍ）

は、互いに素の関係にある整数とするのが望ましい（なお、以下の説明では、Ｎ（１）＜Ｎ（２）＜…＜Ｎ（Ｍ）とする）。この場合に、詳しくは後述するように、想定する最大の結託者数ｃと、シンボル列の要素数Ｍと、使用する識別情報の範囲（例えば、０から始まる連番）との間に、一定の制約を与えるようにしてもよい。

【００６８】

ここで、このＳ（ｉ）＝Ｕ　ｍｏｄ　Ｎ（ｉ）によるシンボル列生成方法について数値を小さくとって簡単にした例を用いて説明する。

【００６９】

例えば、シンボル列の要素の個数Ｍを３とし、Ｎ（１）＝３，Ｎ（２）＝５，Ｎ（３）＝７とする。この場合、第１シンボルＳ（１）は０～２のいずれか、第２シンボルＳ（２）は０～４のいずれか、第３シンボルＳ（３）は０～６のいずれかとなる。

【００７０】

次に、Ｎ（１）×Ｎ（２）×Ｎ（３）－１＝１０４であるので、０～１０４の範囲の全部または一部をユーザＩＤとして用いる。ここでは、そのうち０～１４をユーザＩＤとして用いるものとする。

【００７１】

例えば、ユーザＩＤ＝７の場合、

Ｓ（１）＝７　ｍｏｄ　Ｎ（１）＝７　ｍｏｄ　３＝１、

Ｓ（２）＝７　ｍｏｄ　Ｎ（２）＝７　ｍｏｄ　５＝２、

Ｓ（３）＝７　ｍｏｄ　Ｎ（３）＝７　ｍｏｄ　７＝０、

となる。

【００７２】

また、例えば、ユーザＩＤ＝８の場合、

Ｓ（１）＝８　ｍｏｄ　Ｎ（１）＝８　ｍｏｄ　３＝２、

Ｓ（２）＝８　ｍｏｄ　Ｎ（２）＝８　ｍｏｄ　５＝３、

Ｓ（３）＝８　ｍｏｄ　Ｎ（３）＝８　ｍｏｄ　７＝１、

となる。

【００７３】

図５（ａ）に、この例において各識別情報（ユーザＩＤ＝０～１４）について求められたシンボル列の各序列のシンボルＳ（１），Ｓ（２），Ｓ（３）を示す。

【００７４】

なお、シンボルにアルファベットを用いた場合には、例えば、図５（ｂ）のようになる（なお、図５（ｂ）では、Ｓ（１）＝０にもＳ（２）＝０にもＳ（３）＝０にも全てａを対応させているが、例えば、Ｓ（１）＝０にはａを対応させ、Ｓ（２）＝０にはｂを対応させ、Ｓ（３）＝０にはｃを対応させるような構成も可能である）。

【００７５】

図５（ａ）において、例えば、ユーザＩＤ＝７の場合、Ｓ（１）＝１、Ｓ（２）＝２、Ｓ（３）＝０であるから、ユーザＩＤ＝７に対応するシンボル列は、

｛１，２，０｝

となる。なお、シンボルにアルファベットを用いる場合には、例えば、

｛ｂ，ｃ，ａ｝

となる。

【００７６】

また、例えば、ユーザＩＤ＝８の場合、Ｓ（１）＝２、Ｓ（２）＝３、Ｓ（３）＝１であるから、ユーザＩＤ＝７に対応するシンボル列は、

｛２，３，１｝

となる。なお、シンボルにアルファベットを用いる場合には、例えば、

｛ｃ，ｄ，ｂ｝

となる。

【００７７】

図６に、図５の各識別情報（ユーザＩＤ＝０～１４）に対応するシンボル列を示す（整数を用いた場合と、アルファベットを用いた場合の両方を示す）。

【００７８】

さて、次に、埋め込み符号生成部１２は、シンボル列生成部１１により生成さ

れた、対象複製物に埋め込むべき識別情報（本具体例では、ユーザＩＤ）に対応するシンボル列｛Ｓ（１）、Ｓ（２）、…、Ｓ（Ｍ）｝を受けて、第１シンボルＳ（１）に対応する第１埋め込み符号Ｒ（１）、第２シンボルＳ（２）に対応する第２埋め込み符号Ｒ（２）、…、第Ｍシンボルｓ（Ｍ）に対応する第Ｍ埋め込み符号Ｒ（Ｍ）をそれぞれ生成する（ステップＳ２）。各識別情報に対応するシンボル列の各シンボルに対応する埋め込み符号は、予め生成して記憶しておく方法と、必要時に生成する方法とがある。

【００７９】

ここで、第１シンボルＳ（１）において、第１シンボルＳ（１）の値として取り得る各々の元ｉに対応する第１埋め込み符号w_1（ｉ）は、それぞれ互いに、相互相関が無いようにする（w_1（ｉ）は、第１シンボルにおいて、あるシンボルの元ｉに対応する埋め込み符号を表す）。つまり、ｉ≠ｊならばw_1（ｉ）・w_1（ｊ）＝０、ｉ＝ｊならばw_1（ｉ）・w_1（ｉ）＝１とする。例えば、第１シンボルＳ（１）の取り得る値が｛ａ｝または｛ｂ｝または｛ｃ｝である場合に、第１シンボルＳ（１）＝｛ａ｝に対応する埋め込み符号と、第１シンボルＳ（１）＝｛ｂ｝に対応する埋め込み符号と、第１シンボルＳ（１）＝｛ｃ｝に対応する埋め込み符号とは、いずれの間にも、相互相関が無いようにする。第ｋシンボル（ｋ＝２～Ｍ）についてもそれぞれ同様である（ｉ≠ｊならばw_k（ｉ）・w_k（ｊ）＝０、ｉ＝ｊならばw_k（ｉ）・w_k（ｉ）＝１とする）。なお、相互相関が無いような符号を用いる代わりに、相互相関が非常に小さくなるような符号を用いるようにしてもよい（後者の方が実用的である）。

【００８０】

なお、識別情報に対応するシンボル列を構成する第１～第Ｍシンボルに対応する第１～第Ｍ埋め込み符号をそれぞれコンテンツに埋め込むにあたって、それら第１～第Ｍ埋め込み符号を互いに異なる箇所に埋め込むなど、互いに影響あるいは干渉を及ぼさない形態をとる場合には、互いに他の序列のシンボルに係る埋め込み符号との相互間、すなわち、第１シンボルに用いる埋め込み符号と、第２シンボルに用いる埋め込み符号と、…、第Ｍシンボルに用いる埋め込み符号との相互間には、特に上記のような相互相関についての制約はない。

【００８１】

これに対して、識別情報に対応するシンボル列を構成する第１～第Ｍシンボルに対応する第１～第Ｍ埋め込み符号の全部又は一部の複数のものを同一の箇所に重畳するなど、通常であれば互いに影響あるいは干渉を及ぼし得る形態をとる場合には、それら埋め込み符号については、相互相関が無いようにするか、あるいは相互相関が非常に小さくなるようにするものとする。例えば、第１シンボルに対応する第１埋め込み符号～第Ｍシンボルに対応する第Ｍ埋め込み符号の全てを同一の箇所に重畳する場合には、第１シンボルの全元に対応する埋め込み符号～第Ｍシンボルの全元に対応する埋め込み符号の全ての埋め込み符号の相互間について、相互相関が無いようにするか、あるいは相互相関が非常に小さくなるようにする。

【００８２】

この埋め込み符号としては、種々のものを用いることができる。

【００８３】

例えば、特開２００１－２８５６２３号公報に記載されたシンプレクティック符号を用いることができる。シンプレックス符号とは、符号長ｎ－１、符号語数ｎで、符号語間の相互相関が－１／(ｎ－１)となる符号であり、ｎ次のアダマール(Hadamard)行列を基に構成することができる。すなわち、符号語がｎ－１次元ユークリッド空間中のｎ－１次元単体の頂点に位置するような符号がシンプレックス符号である。例えば、３次元ユークリッド空間の場合は、図７に示すように(-1,-1,1)，(1,-1,-1)，(-1,1,-1)で示す３つの頂点に位置する符号がシンプレックス符号を構成する。

【００８４】

さて、このようにして生成された識別情報に対応するシンボル列の各シンボルにそれぞれ対応する第１～第Ｍ埋め込み符号は、電子透かし埋込装置１の符号埋込部１３が、当該埋め込み符号の内容に従ってコンテンツを予め定められた方法で微少に変更することによって、対象コンテンツに埋め込まれる（ステップＳ３）。なお、コンテンツの変更の仕方には、まず埋め込み対象コンテンツに対して第１埋め込み符号Ｒ（１）を埋め込むようにコンテンツを変更し、次いで、該第

１埋め込み符号Ｒ（１）を埋め込まれたコンテンツに対して第２埋め込み符号Ｒ（２）を埋め込むようにコンテンツを変更し…、というように、逐次的に埋め込みを行う方法や、埋め込み対象コンテンツに対して一挙に全埋め込み符号Ｒ（１）～Ｒ（Ｍ）を埋め込むようにコンテンツを変更するようにする方法や、その他の方法がある。

【００８５】

前述したように、生成された埋め込み符号を対象コンテンツに埋め込む方法（コンテンツのどのような量をどのように変更するか）には、特に限定はなく、どのような方法でも本発明は適用可能である。

【００８６】

ただし、（識別情報に対応するシンボル列の）各シンボルにそれぞれ対応する埋め込み符号は、互いに影響が無いあるいは小さいように、符号構成や埋め込む場所や埋め込み方法等が選択されているようにする。

【００８７】

次に、電子透かし解析装置２について説明する。

【００８８】

ここで、結託攻撃及び結託者の追跡について、数値を小さくとって簡単にした例を用いて説明する。

【００８９】

本実施形態では、結託攻撃として例えば複数の複製物の単純平均操作あるいは重み付け平均操作などを想定している。

【００９０】

例えば、図６のユーザＩＤ＝０，３，１０の各ユーザが入手したコンテンツには、それぞれ、シンボル列として、

｛ａ，ａ，ａ｝

｛ａ，ｄ，ｄ｝

｛ｂ，ａ，ｄ｝

が埋め込まれている。

【００９１】

ここで、上記の３人によって３つのコンテンツ複製物の単純平均操作による結託攻撃が行われたとする。

【００９２】

本実施形態では、識別情報に対応するシンボル列の第１シンボル～第Ｍシンボルのそれぞれにおいて、異なる元に対応する埋め込み符号を互いに相関の無いあるいは非常に小さい電子透かしとして埋め込まれている。しかして、抽出すべきシンボル列における第１シンボル～第Ｍシンボルのそれぞれについて、最大剰余及び最小剰余（＝剰余対）ではなく、埋め込み符号（すなわち、第１埋め込み符号～第M埋め込み符号）を検出し、埋め込み符号をシンボルに戻して、シンボル列を抽出する。ここで、シンボル列における各序列のシンボルをそれぞれ検出するにあたって、結託攻撃に実際に使用されたコンテンツに埋め込まれていた複数のシンボルの元が検出されることがある（上記の具体例では、第１シンボルについて、ａとｂ、第２シンボルについて、ａとｄ、第３シンボルについて、ａとｄが検出され得る）。本実施形態では、第１～第Ｍのシンボルの各々について、結託攻撃に最も数多く用いられたシンボルがいずれかを評価し、最大人口（highest population）と評価されるシンボルを検出し、その検出された最大人口シンボル（highestly populated alphabet）によるシンボル列に基づいて、結託者の識別情報を追跡する。

【００９３】

なお、抽出すべきシンボル列のある序列のシンボルにおいて、最大人口シンボルとなる元が複数存在する場合には、いずれか１つのみを最大人口シンボルとして検出するようにしてもよいし、それら複数を最大人口シンボル（群）として検出するようにしてもよい。

【００９４】

また、最大人口シンボル（群）に加えて、最大人口シンボル以外で検出されたシンボルをも考慮して、追跡を行うようにしてもよい。

【００９５】

上記の具体例の場合、第１～第３のシンボルのそれぞれについて、最も結託に用いられた数の多いシンボルの元が各シンボルの値として検出されるようなシン

ボル列が埋め込まれたコンテンツが作出されることになり、例えば、上記の例では、

｛ａ，ａ，ｄ｝

というシンボル列が埋め込まれたコンテンツ複製物が作出される。この場合、本実施形態の電子透かし解析装置２は、｛ａ，ａ，ｄ｝というシンボル列を検出する。

【００９６】

ここで、図６を見てみると、｛ａ，ａ，ｄ｝というシンボル列に対応する識別情報は存在しない。従って、正当な識別情報が改変されていることがわかる。また、最大人口シンボル以外にも、第１シンボルでは元ｂ、第２シンボルでは元ｄ、第３シンボルでは元ａに対応する埋め込み符号を検出することができるので、このことからも、結託攻撃を受けたことがわかる。

【００９７】

しかして、本実施形態の電子透かし解析装置２は、検出された最大人口シンボルによるシンボル列｛ａ，ａ，ｄ｝（または、これに加えて、最大人口シンボル以外で検出されたシンボル）に基づいて、結託者の識別情報を追跡することができる。

【００９８】

上記した例の場合、追跡アルゴリズム及びその前提となるシンボル列生成方法の構成方法に応じて、例えば、ある誤認識率を含んだ上で、例えばユーザＩＤ＝０のみ（あるいは例えばＩＤ＝０，３，１０の全て）が特定され、あるいは誤認識なしに例えばユーザＩＤ＝０のみ（あるいは例えばＩＤ＝０，３，１０の全て）が特定されることも可能になる。

【００９９】

さて、追跡アルゴリズムとしては、様々なバリエーションが可能であるが、基本的には、抽出されたシンボル列に基づいて、結託攻撃に使用された複製物に埋め込まれていたであろう埋め込み符号／シンボル列に対応するユーザＩＤを求め、これを結託攻撃を行った結託者のユーザＩＤとして特定する。

【０１００】

本実施形態では、結託攻撃後のコンテンツにおいて検出される最大人口によるシンボル列の第ｉシンボルの値は、結託攻撃を行った複数のユーザのうちのいずれかのユーザのユーザＩＤに対応するシンボル列の第ｉシンボルの値に一致する。よって、対象コンテンツから検出された最大人口による埋め込み符号から得られたシンボル列を解析することによって、かりにすべての結託者のユーザＩＤが特定できなかったとしても、一部の結託者のユーザＩＤを特定できることが期待される。

【０１０１】

また、抽出されたシンボル列が、いずれかの正当なユーザに対応するシンボル列と完全に一致する場合には、結託攻撃はなされていないことを特定することができる。ただし、抽出された最大人口によるシンボル列がいずれかの正当なユーザに対応するシンボル列と完全に一致しても、最大人口シンボル以外にも他のシンボルに対応する埋め込み符号が検出されている場合には、結託攻撃を行ったがシンボル列の改変に失敗したことが考えられ、この場合には、特定されたユーザＩＤは、結局、結託攻撃を行っていたことになる。

【０１０２】

追跡アルゴリズムの代表的な種類としては、確率論的方法や決定論的方法などがある。

【０１０３】

確率論的方法は、基本的には、対象コンテンツから検出されたシンボル列から選択された所定数のシンボルが、あるユーザＩＤを示していれば（すなわち、検出シンボル列から選択された所定数のシンボルの値と、あるユーザＩＤに対応する識別情報に対応するシンボル列の同じ序列位置のシンボルの値とがそれぞれ一致すれば）、それを結託者のユーザＩＤとして出力するものである。上記の所定数は、例えば、誤認識率等に応じて決定される（なお、誤認識は、例えば、該選択された所定数のシンボルが実際には一人のユーザにのみ属するものではなく、複数のユーザに分属するものである場合に、結託者でないユーザのユーザＩＤが偶然に出力されてしまうことで生じる）。誤認識をより低く抑えるためには、例えば、上記の所定数をより大きな値に設定すればよい。

【０１０４】

決定論的方法は、基本的には、検出されたシンボル列から、誤認識なしに結託者のユーザＩＤを特定できるようにするものである。すなわち、検出されたシンボル列が結託攻撃によって作出されるために必要不可欠であった結託者のユーザＩＤを解析的に特定するとともに、特定できない場合には追跡不能とする方法である。追跡不能（結託者のユーザＩＤがすべて特定不能）となるケースを０にするまたはより低く抑えるためには、例えば、ユーザＩＤの取り得る値の範囲を一定とした場合にシンボル列の要素数をより多くすればよい。

【０１０５】

図８に、概略的な手順の一例を示す。

【０１０６】

本実施形態の電子透かし解析装置２において、まず、埋め込み符号抽出部２１は、検出対象となるコンテンツの複製物から埋め込み符号Ｒ’（１）、Ｒ’（２）、…、Ｒ’（Ｍ）を抽出する（ステップＳ２１）。そして、シンボル列抽出部２２は、抽出された埋め込み符号Ｒ’（１）、Ｒ’（２）、…、Ｒ’（Ｍ）から、対応するシンボル列｛Ｓ’（１）、Ｓ’（２）、…、Ｓ’（Ｍ）｝を求める（ステップＳ２２）。

【０１０７】

図９に、埋め込み符号抽出部２１の処理手順の一例を示す。

【０１０８】

埋め込み符号抽出部２１は、追跡対象となるコンテンツの複製物から抽出すべきシンボル列の各シンボルＳ’（１）、Ｓ’（２）、…、Ｓ’（Ｍ）にそれぞれ対応する埋め込み符号Ｒ’（１）、Ｒ’（２）、…、Ｒ’（Ｍ）の各々について、当該埋め込み符号Ｒ’（ｉ）として使用されている可能性のある各符号（すなわち、シンボルＳ’（ｉ）の各元にそれぞれ対応する各埋め込み符号）の評価値をそれぞれ求め（評価値計算処理）（ステップＳ３１）、各埋め込み符号Ｒ’（ｉ）ごとに、求めた各符号の表価値に基づいて、第ｉの埋め込み符号を決定する（ＨＰＥ（Highestly Populated Elements）計算処理）（ステップＳ３２）。

【０１０９】

ここで、平均による結託攻撃の場合、Ω（（Ｌ／ln　ｎ）$^{1/2}$）人の結託によって電子透かしの消去が行えるという解析結果がある（例えば文献１「J.Kilian, F.T.Leighton, T.G.Shamoon, R.E.Tarjan and F.Zane, “Resistance of Digital Watermarks to Collusive Attacks”, NEC Research Institute, Technical Report TR-585-98, 1998.」）。ここで、Ｌはコンテンツのサイズ（電子透かしを埋め込める容量）、ｎは配布先となるユーザの総数とする。これより、最大結託サイズをｃとすれば、長さＬ（Ｌはｃ^{2}・ln　ｎに比例する値）のコンテンツが必要となるため、ｃが大きくなると電子透かしが失われる。この解析は、電子透かしがランダムなガウシアンノイズとして重畳されることを仮定しており、平均による結託攻撃により電子透かしの平均は、中心極限定理によりｃが大きくなると０になる。

【０１１０】

そこで、本実施形態では、前述したように、各ユーザＩＤに対応するシンボル列における第ｉシンボル（ｉ＝０～Ｍ）に対して、Ｎ（ｉ）個の元の集合＝｛$a_{i,0}$, $a_{i,1}$, …, $a_{i,N(i)-1}$｝のうちから選択した１つの元$a_{i,j}$に対応する埋め込み符号$r_{i,j}$（$r_{i,j}$は他の元$a_{i,k}$（ｋ≠ｊ）に対応する埋め込み符号$r_{i,k}$（ｋ≠ｊ）との間に相関の無いあるいは非常に小さい埋め込み符号）を電子透かしとして埋め込み、平均による結託攻撃が行われた場合には、剰余対（＝最大剰余及び最小剰余）の集合ではなく、最大人口による第ｉシンボルを検出し、最大人口シンボルからなる抽出シンボル列を検出する方法をとっている。

【０１１１】

例えば文献１の解析では、電子透かしが一般的なガウシアンノイズとしてモデルされているが、この方法では、そのようなガウシアンノイズの成す空間のうち、非常に限定された（例えば、Ｎ（ｉ）次元の）部分空間の中にしか電子透かしが値を取らない。しかも、それぞれの成分が直交しているため、平均をとっても、複数の電子透かしが相殺しあうことはない。

【０１１２】

最大人口シンボルに対応する埋め込み符号の抽出は、例えば、次のように行うことができる。

【０１１３】

抽出すべきシンボル列における第ｉシンボルに対して、上記の評価値計算処理として、各元$a_{i,j}$（ここで、ｊ＝０～Ｎ（ｉ－１））に対して相互相関の無い埋め込み符号$m_{i,j}$が対応している（つまり、$m_{i,j}\cdot m_{i,k}=\delta_{j\cdot k}$とする）。第ｉシンボルについて、コンテンツＩと、第ｉシンボルにおける各元$a_{i,j}$に対応する埋め込み符号$m_{i,j}$との相互相関$C_{i,j}=m_{i,j}\cdot I$を測定する。この相関値$C_{i,j}$を、第ｉシンボルに対応する第ｉ埋め込み符号における当該符号$m_{i,j}$の評価値とする。この値$C_{i,j}$が最大となるjmaxに係る埋め込み符号$m_{i,jmax}$が、第ｉ埋め込み符号における最大人口シンボルに対応する埋め込み符号であり、これに対応する第ｉシンボルの元$a_{i,jmax}$が、求めるべき第ｉシンボルの最大人口シンボルとなる。

【０１１４】

図１０は、抽出すべきシンボル列のある序列のシンボル（第１シンボルとする）に係る最大人口シンボルの決定を説明するための図である。第１シンボルの各元（本例では、ａ，ｂ，ｃ）にそれぞれ対応する第１の埋め込み符号の候補としての各符号についてそれぞれ求めれらた評価値を、ベクトルｖで表すものとする。図１０において、各軸は、第１シンボルの元に対応する。ベクトルｖの方向が最も近い軸に対応する元を、求めるべきシンボル列における第１シンボルとして出力する。

【０１１５】

例えば、図１１（ａ）のように、単純平均化法による結託攻撃に使用されたコンテンツの複製物の数が１００（あるいは、重み付け平均化法による重みを考慮した延べ数が１００）であり、第１シンボルにおいて、元$a_{1,1}$，$a_{1,2}$，$a_{1,3}$，$a_{1,4}$に対応する人口（結託攻撃に使用された当該元に係るコンテンツの複製物の数）がそれぞれ、５３，２３，８，１３であったとすると、最大人口の第１シンボル$a_{1,1}$に対応する埋め込み符号$r_{1,1}$が、埋め込み符号抽出部２１によって求められる。そして、シンボル列抽出部２２は、抽出された第１の埋め込み符号$r_{1,1}$を受け、これに対応するシンボル$a_{1,1}$を第１シンボルとする。同様にして、最大人口による第２～第Ｍシンボルが求められ、抽出すべきシンボル列が得

られる。なお、結託攻撃に使用されたコンテンツの複製物に埋め込まれている識別情報の組み合わせによっては、図１１（ｂ）のように、ほとんど１つのシンボルに偏ることも、唯一のシンボルに偏ることもあり得る。

【０１１６】

なお、前述したように、抽出すべきシンボル列のある序列のシンボルにおいて、最大人口シンボルとなる元が複数存在する場合には、いずれか１つのみを最大人口シンボルとして検出するようにしてもよいし、それら複数を最大人口シンボル（群）として検出するようにしてもよい。

【０１１７】

また、最大人口シンボル（群）に加えて、最大人口シンボル以外で検出されたシンボルをも考慮して、追跡を行うようにしてもよい。

【０１１８】

次いで、追跡部２３は、抽出されたシンボル列｛Ｓ’（１）、Ｓ’（２）、…、Ｓ’（Ｍ）｝に対して、追跡アルゴリズムを実行する（ステップＳ２３）。

【０１１９】

まず、確率論的方法による追跡アルゴリズムの一例について説明する。

【０１２０】

最大人口シンボル（群）からなるシンボル列に基づいて確率論的に結託者を特定する方法は、例えば、ｃ－ｓｅｃｕｒｅ　ＣＲＴ符号において、マーキング仮定を変更することで得られる。ここでは、第ｉシンボルにおいて、最大人口シンボルとしてある元$a_{i,j}$が検出される確率は、１／Ｎ（ｉ）であるという仮定をおく。これは、結託がランダムに構成されるとすれば妥当な仮定である（あるいは、第ｉシンボル内でシンボルの元の間でランダムな置換を行うこととし、検出時の確率は、すべてのランダムな置換にわたってとることとすれば、妥当な仮定となる）。

【０１２１】

図１２に、この場合の処理手順の一例を示す。

【０１２２】

まず、すべてのユーザＩＤ（＝U_iとする）について、Ｄ（U_i）を求める（ス

テップＳ４１）。

【０１２３】

ここで、Ｄ（U_i）は、該ユーザＩＤ＝U_iのユーザに割り当てられるシンボル列｛Ｓ（１）、Ｓ（２）、…、Ｓ（Ｍ）｝＝｛U_i ｍｏｄ Ｎ（１）、U_i ｍｏｄ Ｎ（２）、…、U_i ｍｏｄ Ｎ（Ｍ）｝と、抽出されたシンボル列｛Ｓ’（１）、Ｓ’（２）、…、Ｓ’（Ｍ）｝とを、両シンボル列で同一の序列に位地するもの同士でそれぞれ比較した場合に、一致したシンボルの個数を表す。

【０１２４】

次に、各ユーザＩＤ＝U_iに対して求めたＤ（U_i）について、当該Ｄ（U_i）と、あらかじめ定められたしきい値D_{th}とを比較し、Ｄ（U_i）≧D_{th}ならば、そのユーザＩＤ＝U_iを、結託者のユーザＩＤと特定する（ステップＳ４２）。

【０１２５】

なお、D_{th}は、例えば、D_{th}＝ｋ＋１で、ｋは、Ｎ（０），…，Ｎ（ｋ）の積を、ユーザＩＤ（識別情報）の総数以上とするような値（ここで、Ｎ（０）≦Ｎ（１）≦…≦Ｎ（Ｍ）とする）であり、１は、例えば、式（１）で与えられる。

$$[1-\Pi\ 1/N(i)]^{S} \geqq 1-\varepsilon_2 \qquad (1)$$

ここで、Πをとるｉの範囲は、ｉ＝０～（１－１）あるいはｉ＝ｋ～（ｋ＋１－１）、

$S = {}_{M}C_{k+1}$、

ε_2は、結託者のユーザＩＤ（識別情報）における追跡誤り率で、０＜ε２＜１を満たす。

【０１２６】

例えば、前述の具体例において、図６のユーザＩＤ＝０，３，１０の各ユーザが入手したコンテンツには、それぞれ、シンボル列として、

｛ａ，ａ，ａ｝

｛ａ，ｄ，ｄ｝

｛ｂ，ａ，ｄ｝

が埋め込まれており、それら３人によって３つのコンテンツ複製物の単純平均操

作による結託攻撃が行われて、

｛ａ，ａ，ｄ｝

というシンボル列が埋め込まれたコンテンツ複製物が作出されたものとする。

【０１２７】

ここで、｛ａ，ａ，ｄ｝という抽出シンボル列が得られたとする。

【０１２８】

ユーザＩＤ＝０について、これに固有に割り当てられたシンボル列と、抽出シンボルとを比較すると、第１シンボルはいずれも｛ａ｝で一致し、第２シンボルはいずれも｛ａ｝で一致し、一方、第３シンボルは｛ａ｝と｛ｄ｝で一致しないので、この場合、Ｄ（０）＝２となる。同様に、Ｄ（３）＝２、Ｄ（１０）＝２となる。

【０１２９】

ここで、かりにD_{th}＝２ならば、図６のユーザＩＤ＝０～１４のうち、ユーザＩＤ＝０，３，１０の３人のみが、Ｄ（０）≧D_{th}、Ｄ（３）≧D_{th}、Ｄ（１０）≧D_{th}を満たすので、この場合には、ユーザＩＤ＝０，３，１０が、結託者のユーザＩＤとして特定される。

【０１３０】

ここで、従来のｃ－ｓｅｃｕｒｅ　ＣＲＴ符号は、各内符号が複数のブロックで構成され、各ブロックのビット反転を観測することで、最大剰余及び最小剰余を検出しており、さらにブロックを構成する各ビットは、例えば、電子透かしとして埋め込まれることを想定していたのに対して、本実施形態では、シンボル列の元が電子透かしとして埋め込まれており、最大人口シンボルを検出することで、内符号感度の問題を軽減できるとともに、符号の構成が単純になったため符号長の短縮にもつながる。前述したように、外符号としては、ｃ－ｓｅｃｕｒｅ　ＣＲＴ符号の外符号のマーキング仮定の変更を反映したｃ－ｓｅｃｕｒｅ性のための条件から決定された個数の内符号を用意することで、ｃ－ｓｅｃｕｒｅ　ＣＲＴ符号と同様の追跡が行える。

【０１３１】

ここで、文献２「Y.Yacobi，“Improved Boneh-Shaw content fingerprinting

”，Topics in Cryptology - C-RSA 2001，378-391，2001.」に提案されている方法との差異を述べておく。文献２では、内符号のブロックを電子透かしで置き換える方法を提案している。この場合、最大剰余及び最小剰余を求める内符号感度の問題は解決されていない。しかし、文献２では、外符号として、文献３「D. Boneh and J.Shaw，“Collusion-Secure Fingerprinting for Digital Data”，Advance in Cryptology: Proceedings of CRYPTO' 95，Springer-Verlag，452-465，1995.」や文献４「D.Boneh and J.Shaw，“Collusion-Secure Fingerprinting for Digital Data”，IEEE Transactions on Information Theory，44，5，1897-1905，1998.」で提案されているような誤り訂正符号を用いた外符号、あるいは、ランダム符号による符号の構成を前提としている。これらの外符号では、最大剰余及び最小剰余は必要ではなく、剰余の中から１つ検出できていればよい。ただし、この外符号は、Ｏ（$c^2 \cdot \log n$）の長さを持つことから、ｃが大きくなると急速に符号長が大きくなる。

【０１３２】

次に、決定論的方法による追跡アルゴリズムの一例について説明する。

【０１３３】

決定論的方法による追跡アルゴリズムは、例えば、文献５「H.Muratani，“Combination Outer Codes for c-secure CRT Codes”，SCIS2002，13D-3，2002.」の方法を利用することができる。この場合、想定する最大の結託者数ｃが大きいときは埋め込み符号の符号長をある程度符号長を長くするのが好ましいが、ｃが小さいときは確率論的方法による追跡アルゴリズムにおける埋め込み符号よりも短い符号長で済むことになる。

【０１３４】

誤検出を０または非常に小さくするために、想定する最大の結託者数ｃと、シンボル列の要素数Ｍと、使用する識別情報の範囲（例えば、０から始まる連番）との間に、一定の制約を与えるようにしてもよい。例えば、$M > c^2 \cdot (K-1)$とするようにしてもよい。

【０１３５】

ここで、追跡アルゴリズムでは、結託攻撃が行われる際の最大結託数をｃと想

定する。すなわち、２≦ａ≦ｃを満たす任意のａ人の結託者すなわちａ個の相互に異なる識別情報の埋め込まれたコンテンツの複製物により結託攻撃が行われる場合を考える（なお、ここでは、ユーザと識別情報とが１対１に対応するものとして考えているが、例えば、ユーザと識別情報とが１対多対応となり得る場合であって、実際に同一の結託者が自身に対応する２つの識別情報をそれぞれ埋め込まれた同一のコンテンツについての２つの複製物を当該結託攻撃に供する際には、結託者の数とは、異なる識別情報を埋め込まれたコンテンツの複数物ごとに考えることになる）。

【０１３６】

以下では、ａ（２≦ａ≦ｃ）個の相互に異なる識別情報の埋め込まれたコンテンツの複製物により結託攻撃を行う際に供される当該複数のコンテンツの複製物にそれぞれ埋め込まれた識別情報により構成される識別情報群を、結託者グループと呼ぶものとする。例えば、図６の例では、識別情報＝ユーザＩＤ＝０～１４であるので、最大結託数ｃ＝３とすると（実際には識別情報の範囲や最大結託数はもっと大きく取られる）、結託者グループには、｛０，１｝、｛０，２｝、…、｛０，１４｝、｛１，１｝、｛１，２｝、…、｛１，１４｝、｛２，３｝、…｛２，１４｝、｛３，４｝、…、｛１１，１４｝、｛１２，１３｝、｛１２，１４｝、｛１３，１４｝（以上、ａ＝２による結託）、｛０，１，２｝、｛０，１，３｝、…、｛０，１，１４｝、｛０，２，３｝、｛０，２，４｝、…、｛０，２，１４｝、｛０，３，４｝、…、｛１０，１１，１４｝、｛１１，１２，１３｝、｛１１，１２，１４｝、｛１２，１３，１４｝（以上、ａ＝３による結託）がある。最大結託数ｃ＝３以下での結託攻撃は、必ず、上記の結託者グループのいずれかによって行われる。

【０１３７】

次に、追跡対象コンテンツから抽出された抽出シンボル列を入力し、これに適合する結託者グループを出力する。

【０１３８】

ここで、ある結託者グループが抽出シンボル列に適合するとは、次の場合である。すなわち、その結託者グループを構成する複数の識別情報の各々に固有に対

応するシンボル列を基にして、何らかの結託による操作（例えば平均操作）により、当該抽出シンボル列が作出され得るものと判断される場合に、当該ある結託者グループが、当該抽出シンボル列に適合すると判断する。

【０１３９】

例えば、図６の具体例において、あるコンテンツから、

｛ａ，ａ，ｄ｝

というシンボル列が抽出された場合に、前述の図６のユーザＩＤ＝０，３，１０からなる結託者グループは、当該抽出シンボル列｛ａ，ａ，ｄ｝に適合することになる。

【０１４０】

適合する結託者グループの数は、抽出シンボル列の内容によって、１つになる場合と、複数になる場合とがあり得る。

【０１４１】

なお、抽出されたシンボル列が、いずれかの正当なユーザに対応するシンボル列と完全に一致し、かつ、最大人口シンボル以外のシンボルが存在しない場合には、結託攻撃はなされていないことを特定することができる。ただし、抽出された最大人口によるシンボル列がいずれかの正当なユーザに対応するシンボル列と完全に一致しても、最大人口シンボル以外にも他のシンボルに対応する埋め込み符号が検出されている場合には、結託攻撃を行ったがシンボル列の改変に失敗したことが考えられ、この場合には、特定されたユーザＩＤは、結局、結託攻撃を行っていたことになる。

【０１４２】

また、何らかの理由により、適合する結託者グループが得られない場合は、、エラーとなる。

【０１４３】

さて、次に、抽出シンボル列に対して、１つの結託者グループのみが得られた場合には、該結託者グループを構成する識別情報を全て、結託者の識別情報とすればよい。

【０１４４】

一方、２以上の結託者グループが得られた場合には、得られた全ての結託者グループに共通に存在する（１又は複数の）識別情報のみを、結託者の識別情報とすればよい。なお、この共通に存在する識別情報を、共通識別情報と呼ぶものとする。

【０１４５】

ここで、同一の剰余対表現から複数の結託者グループが得られた場合には、いずれの結託者グループが、実際に結託攻撃に参加したであろう結託者のユーザＩＤ（識別情報）に対応するものかは、（抽出シンボル列のみからは）わからない。しかし、（結託攻撃が最大結託者数以下の結託者数で行われたとすれば）、それらのうちのいずれか１つの結託者グループが、求めるべき結託者グループである。したがって、得られた複数の結託者グループの全てに共通に存在する識別情報があれば、少なくともその識別情報（すなわち共通識別情報）は、実際に結託攻撃に参加したであろう結託者の識別情報である。

【０１４６】

なお、２以上の結託者グループが得られた場合であっても、共通識別情報が１つもないときは、特定不能とする。なお、得られた複数の結託者グループに共通識別情報が存在しないケースが理論的には発生しないように構成した場合には、得られた複数の結託者グループに共通識別情報が存在しないケースは何らかのエラーによってのみ発生することになる。

【０１４７】

このように、実際に結託攻撃に参加したであろう結託者が、たとえ全ては分からなくても、確実に一人でも分かるということは、デジタルコンテンツの違法コピーに対する事前の抑制や著作権侵害が発生したときの事後の救済のために、非常に大きな意味がある。

【０１４８】

ところで、複数の結託者グループが得られたものの共通識別情報が存在しないケースは、できるだけ少なく抑えらるのが望ましい。そして、このようなケースは、何らかの手段によって、少なくすることができる。

【０１４９】

例えば、複数の結託者グループが得られたものの、共通識別情報が存在しないようなケースを探索し、そのような結託者グループを構成する識別情報の全部又は一部を使用しないようにすることも、一つの方法である。

【０１５０】

また、例えば、想定する最大の結託者数ｃを一定とすれば、定性的には、整数の個数Ｍ（＝成分符号の個数）を増加させるほど、あるいは使用する識別情報の範囲を減少させるほど、上記のケースを少なくすることができる。

【０１５１】

図１３に、この場合の処理手順の一例を示す。

【０１５２】

まず、与えられた抽出シンボル列に適合する結託者グループを全て求める（ステップＳ５１）。

【０１５３】

求められた結託者グループの数が１である場合（ステップＳ５２）、求められた結託者グループを構成する全てのユーザＩＤを結託者のユーザＩＤ（結託者ＩＤ）とし（ステップＳ５３）、求められた結託者ＩＤを出力する（ステップＳ５６）。

【０１５４】

求められた結託者グループの数が２以上である場合（ステップＳ５２）、求められた全ての結託者グループに共通に存在するユーザＩＤがあれば（ステップＳ５４）、求められた全ての結託者グループに共通に存在する（１又は複数の）ユーザＩＤのみを結託者ＩＤとし（ステップＳ５５）、求められた結託者ＩＤを出力する（ステップＳ５６）。一方、求められた全ての結託者グループに共通に存在するユーザＩＤがなければ（ステップＳ５４）、結託者ＩＤが得られなかった旨（またはその旨及び結託者グループを特定する情報、またはその旨及び抽出シンボル列）を出力する（ステップＳ５７）。

【０１５５】

なお、ステップＳ２で結託者グループが１つも得られない場合には、エラーとなる。

【０１５６】

なお、ユーザＩＤの総数が大きい場合には、全ての結託者グループに対して、この処理を行うことは、コストが大きいので、例えば、結託者グループのサイズに関する条件や、現実の結託攻撃がそれを破る確率は十分に小さいと考えられる条件などによって、限定された結託者グループに対してのみ、この処理を行うようにしてもよい。

【０１５７】

さて、符号の構成方法としては、誤り訂正符号をｃ－ｓｅｃｕｒｅ　ＣＲＴ符号の外符号に用いる方法もある。この場合にも、決定論的な追跡を行う方法と、確率論的な追跡を行う方法がある。決定論的な追跡を行う外符号については、文献３，文献４，文献６「B.Chor, A.Fiat and M.Naor, “Tracing Traitors”, Advances in Cryptology-CRYPTO’ 94, LNCS 839, 257-270, 1994.」，文献７「H.D.L.Hollmann, J.H.van Lint, J.-P.Linnartz and L.M.G Tolhuizen, “On codes with the indentifiable parent property”, Jounal of Combinatorial Theory, 82, 121-133, 1998.」，文献８「J.N.Staddon, D.R.Stinson and R.Wei, “Combinational Properties of frameproof and treacability code”, 2000.」，文献９「R.Safavi-Naini and Y.Wang, “Collusion Secure q-ary Fingerprinting for Perceptual Content”, Warkshop on Security and Privacy in Digital Rights Management 2001, November, 2001.」に符号の提案がある。

【０１５８】

確率論的な追跡については、従来のｃ－ｓｅｃｕｒｅ　ＣＲＴ符号（例えば、文献１０「H.Muratani, “Collusion Resilience of digital watermarking”, SCSI2000, C06, 2000.」や文献１１「H.Muratani, “Collusion-Secure Fingerprinting Code Reduced by Chinese Remaindering and its Random-Error Resilisence”, infomation hiding, Proceedings of the 4th International Workshop, IH 2001, 303-315, 2001.」）の外符号の拡張を行うことで構成できる。

【０１５９】

以下、Ｒｅｅｄ－Ｓｏｌｏｍｏｎ符号を使った例を説明する。

【０１６０】

ここで、Ｎ＝ｃ（ｋ＋１）とする。Ｃをｎａｒｒｏｗ　ｓｅｎｓｅ［Ｎ，ｋ，Ｎ－ｋ＋１］$_{q}$　Ｒｅｅｄ－Ｓｏｌｏｍｏｎ符号とする。

【０１６１】

次の式（２）の条件が満たされるとき、この符号は、確率論的外符号とできる。

$$[1-1/q^{l}]^{S} \geqq 1-\varepsilon \qquad (2)$$

ここで、$S={}_{M}C_{k+l}$、

ｑ＝Ｎ（０）＝Ｎ（１）＝…＝Ｎ（Ｍ）、

εは、結託者のユーザＩＤ（識別情報）における追跡誤り率で、０＜ε＜１なる実数とする。

【０１６２】

この場合に、先に例示した確率論的方法による追跡アルゴリズムの一例を適用することも可能である。なお、この場合には、先に例示した確率論的方法による追跡アルゴリズムの一例で、しきい値D_{th}＝ｋ＋１において、ｌは、式（１）の代わりに、例えば、式（２）で与えられるものとしてもよい。

【０１６３】

もちろん、この場合に、先に例示した決定論的方法による追跡アルゴリズムの一例を適用することも可能である。

【０１６４】

この符号は、ＡＧ（Ａｌｇｅｂｒａｉｃ　Ｇｅｏｍｅｔｙｒ）符号をベースにした構成も可能である。

【０１６５】

以下では、本実施形態のハードウェア構成、ソフトウェア構成について説明する。

【０１６６】

本実施形態の電子透かし解析装置は、ハードウェアとしても、ソフトウェア（（コンピュータに所定の手段を実行させるための、あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための）プログラム）としても、実現可能である。また、電子透かし解析装置

をソフトウェアで実現する場合には、記録媒体によってプログラムを受け渡しすることも、通信媒体によってプログラムを受け渡しすることもできる。もちろん、それらは、電子透かし埋込装置についても同様である。

また、電子透かし埋込装置や電子透かし解析装置をハードウェアとして構成する場合、半導体装置として形成することができる。

また、本発明を適用した電子透かし解析装置を構成する場合、あるいは電子透かし解析プログラムを作成する場合に、同一構成（あるいは、共有もしくは使い回し可能な構成）を有するブロックもしくはモジュールがあっても、それらをすべて個別に作成することも可能であるが、同一構成（あるいは、共有もしくは使い回し可能な構成）を有するブロックもしくはモジュールについては１または適当数のみ用意しておいて、それをアルゴリズムの各部分で共有する（使い回す）ことも可能である。電子透かし埋込装置を構成する場合、あるいは電子透かし埋め込みプログラムを作成する場合も、同様である。また、電子透かし埋込装置および電子透かし解析装置を含むシステムを構成する場合、あるいは電子透かし埋め込みプログラムおよび電子透かし検出プログラムを含むシステムを作成する場合には、電子透かし埋込装置（あるいはプログラム）と電子透かし解析装置（あるいはプログラム）に渡って、同一構成（あるいは、共有もしくは使い回し可能な構成）を有するブロックもしくはモジュールについては１または適当数のみ用意しておいて、それをアルゴリズムの各部分で共有する（使い回す）ことも可能である。

【０１６７】

また、電子透かし埋込装置や電子透かし解析装置をソフトウェアで構成する場合には、マルチプロセッサを利用し、並列処理を行って、処理を高速化することも可能である。

【０１６８】

また、これまで説明してきた構成は、装置の一部としてだけでなく、それ自体が一つの装置として成立可能である。例えば、電子透かし解析装置の復号部２２は、電子透かし解析装置を構成する一体不可分の構成部分としても、電子透かし解析装置を構成する部品あるいはモジュール等としも、独立した復号装置として

も成立する。

【０１６９】

なお、この発明の実施の形態で例示した構成は一例であって、それ以外の構成を排除する趣旨のものではなく、例示した構成の一部を他のもので置き換えたり、例示した構成の一部を省いたり、例示した構成に別の機能あるいは要素を付加したり、それらを組み合わせたりすることなどによって得られる別の構成も可能である。また、例示した構成と論理的に等価な別の構成、例示した構成と論理的に等価な部分を含む別の構成、例示した構成の要部と論理的に等価な別の構成なども可能である。また、例示した構成と同一もしくは類似の目的を達成する別の構成、例示した構成と同一もしくは類似の効果を奏する別の構成なども可能である。

また、この発明の実施の形態で例示した各種構成部分についての各種バリエーションは、適宜組み合わせて実施することが可能である。

また、この発明の実施の形態は、個別装置としての発明、関連を持つ２以上の装置についての発明、システム全体としての発明、個別装置内部の構成部分についての発明、またはそれらに対応する方法の発明等、種々の観点、段階、概念またはカテゴリに係る発明を包含・内在するものである。

従って、この発明の実施の形態に開示した内容からは、例示した構成に限定されることなく発明を抽出することができるものである。

【０１７０】

本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【０１７１】

【発明の効果】

本発明によれば、結託攻撃に用いられたコンテンツの複製物に埋め込まれていたであろう識別情報を、より感度の高い符号によって推定することができるようになる。

【図面の簡単な説明】

【図１】

本発明の一実施形態に係る電子透かし埋込装置及び電子透かし解析装置を含むコンテンツ流通システムの概略構成を示す図

【図２】

同実施形態に係る電子透かし埋込装置の構成例を示す図

【図３】

同実施形態に係る電子透かし解析装置の構成例を示す図

【図４】

同実施形態に係る電子透かし埋込装置の概略的な手順の一例を示すフローチャート

【図５】

同実施形態に係る識別情報とシンボル列の具体例について説明するための図

【図６】

同実施形態に係る識別情報とシンボル列の具体例について説明するための図

【図７】

シンプレックス符号について説明するための図

【図８】

同実施形態に係る電子透かし解析装置の概略的な手順の一例を示すフローチャート

【図９】

同実施形態に係る埋め込み符号抽出部の処理手順の一例を示すフローチャート

【図１０】

同実施形態に係る最大人口シンボルについて説明するための図

【図１１】

同実施形態に係る最大人口シンボルについて説明するための図

【図１２】

同実施形態に係る追跡部の処理手順の一例を示すフローチャート

【図１３】

同実施形態に係る追跡部の処理手順の他の例を示すフローチャート

【符号の説明】

１…電子透かし埋込装置

２…電子透かし解析装置

３…流通経路

１１…シンボル列生成部

１２…埋め込み符号生成部

１３…符号埋込部

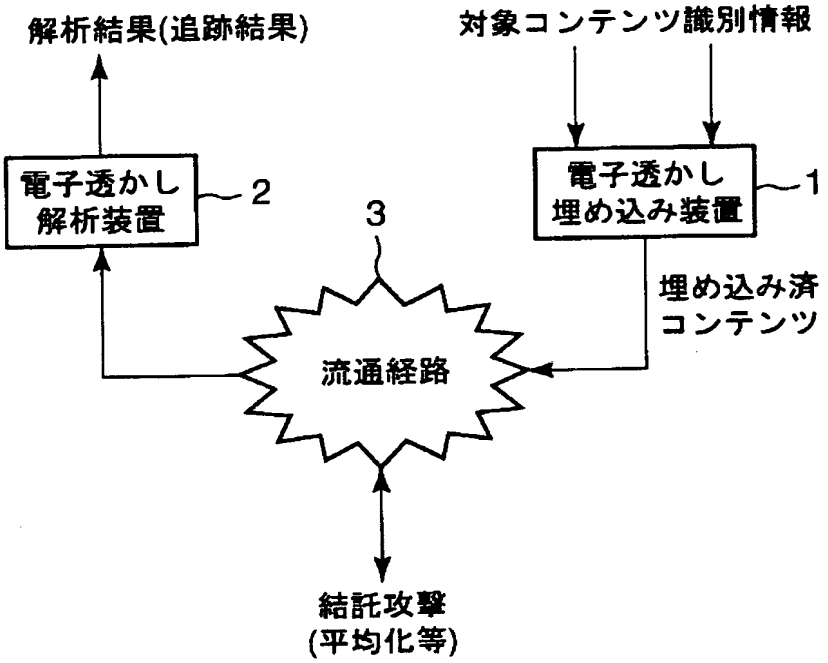
２１…埋め込み符号抽出部

２２…シンボル列抽出部

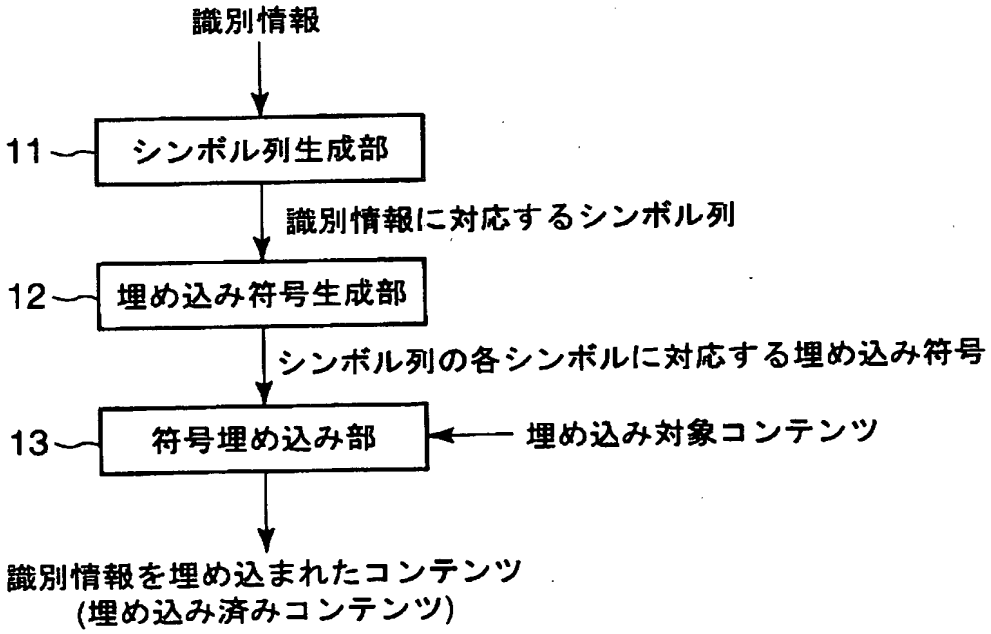
２３…追跡部

【書類名】　図面

【図１】

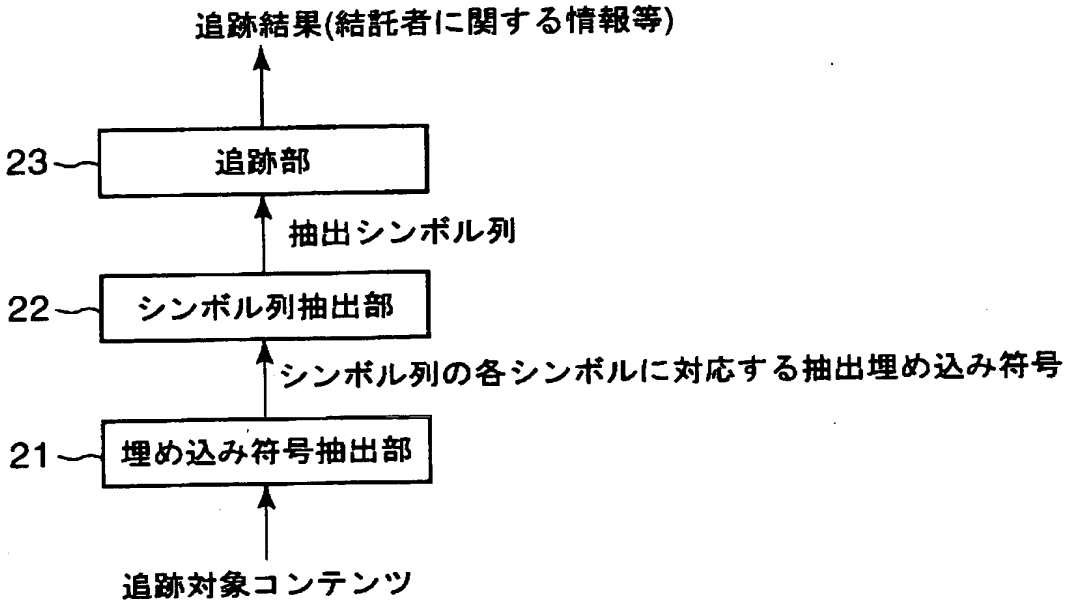


【図２】

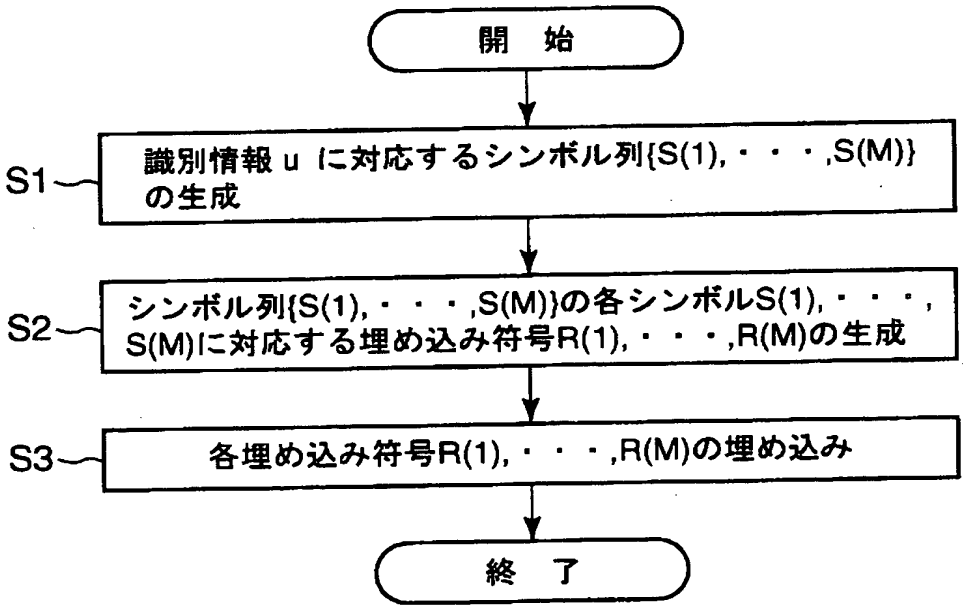


出証特２００３－３００２７９４

【図３】


追跡結果(結託者に関する情報等)
23
追跡部
抽出シンボル列
22
シンボル列抽出部
シンボル列の各シンボルに対応する抽出埋め込み符号
21
埋め込み符号抽出部
追跡対象コンテンツ

【図４】


開　始
S1
識別情報 u に対応するシンボル列{S(1),・・・,S(M)}の生成
S2
シンボル列{S(1),・・・,S(M)}の各シンボルS(1),・・・,S(M)に対応する埋め込み符号R(1),・・・,R(M)の生成
S3
各埋め込み符号R(1),・・・,R(M)の埋め込み
終　了

【図５】

ID	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
S(1)	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2
S(2)	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4
S(3)	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0

(a)

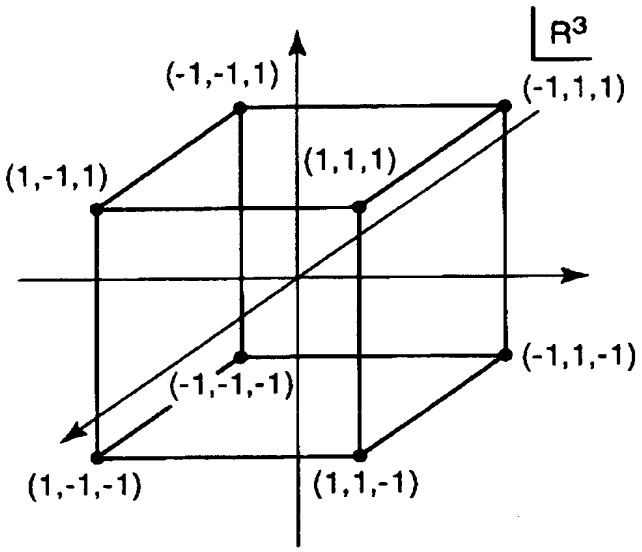
ID	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
S(1)	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c
S(2)	a	b	c	d	e	a	b	c	d	e	a	b	c	d	e
S(3)	a	b	c	d	e	f	g	a	b	c	d	e	f	g	a

(b)

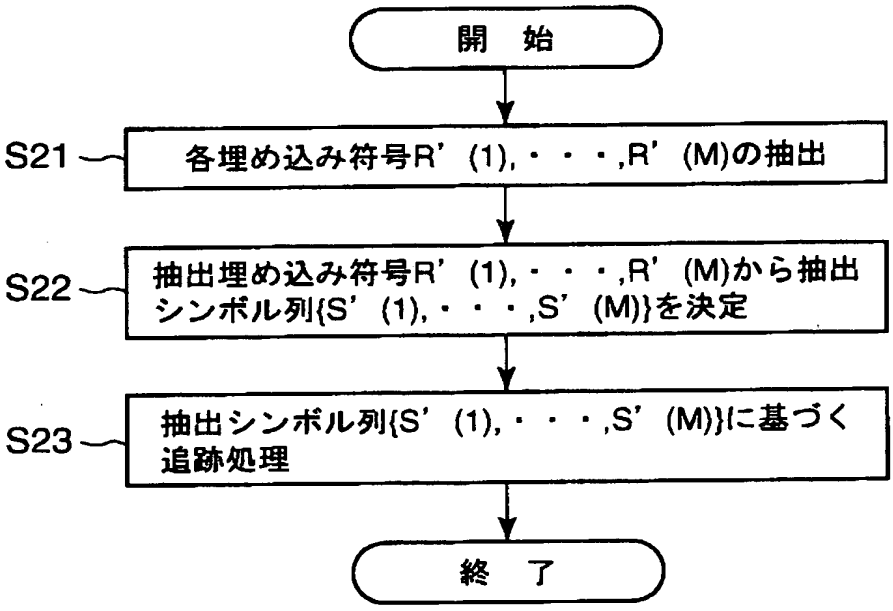
【図６】

ユーザ ID	ユーザ ID に対応するシンボル列	
0	{0,0,0}	{a,a,a}
1	{1,1,1}	{b,b,b}
2	{2,2,2}	{c,c,c}
3	{0,3,3}	{a,d,d}
4	{1,4,4}	{b,e,e}
5	{2,0,5}	{c,a,f}
6	{0,1,6}	{a,b,g}
7	{1,2,0}	{b,c,a}
8	{2,3,1}	{c,d,b}
9	{0,4,2}	{a,e,c}
10	{1,0,3}	{b,a,d}
11	{2,1,4}	{c,b,e}
12	{0,2,5}	{a,c,f}
13	{1,3,6}	{b,d,g}
14	{2,4,0}	{c,e,a}

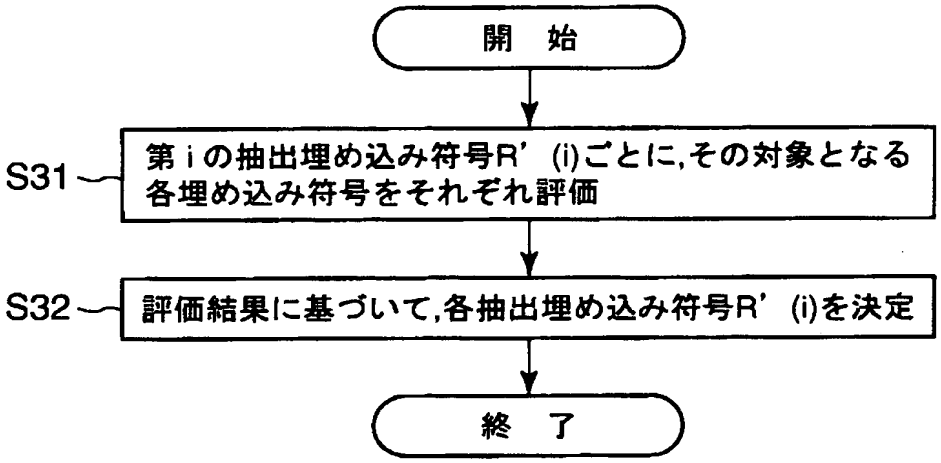
【図７】


R3
(-1,-1,1)
(-1,1,1)
(1,-1,1)
(1,1,1)
(-1,1,-1)
(-1,-1,-1)
(1,-1,-1)
(1,1,-1)

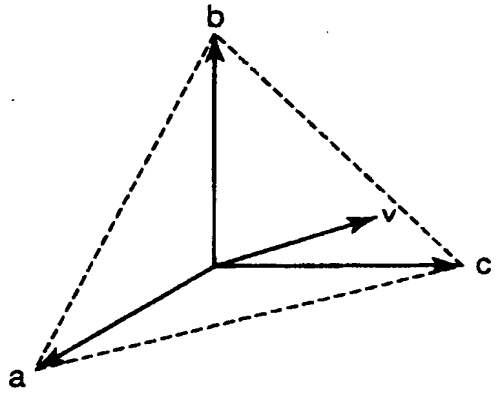
【図８】


開　始
S21
各埋め込み符号R'(1),・・・,R'(M)の抽出
S22
抽出埋め込み符号R'(1),・・・,R'(M)から抽出
シンボル列{S'(1),・・・,S'(M)}を決定
S23
抽出シンボル列{S'(1),・・・,S'(M)}に基づく
追跡処理
終　了

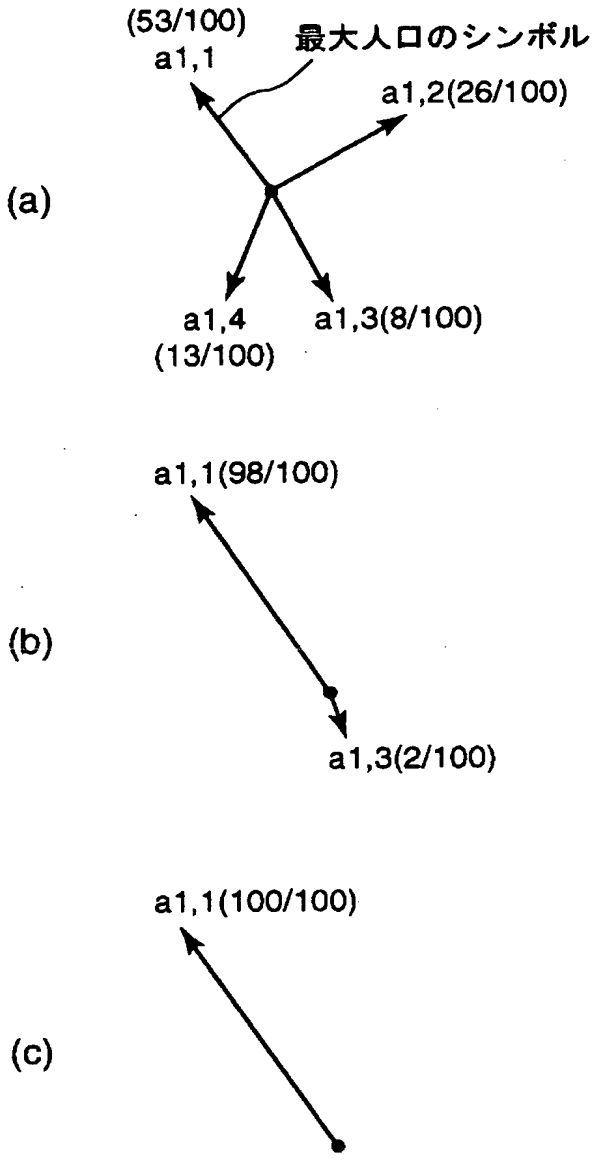
【図９】


開　始
S31
第ｉの抽出埋め込み符号R'(i)ごとに,その対象となる各埋め込み符号をそれぞれ評価
S32
評価結果に基づいて,各抽出埋め込み符号R'(i)を決定
終　了

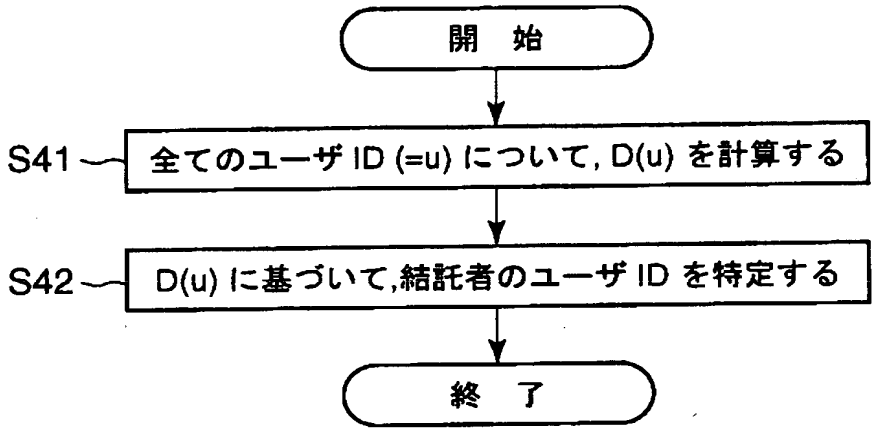
【図１０】


b
v
c
a

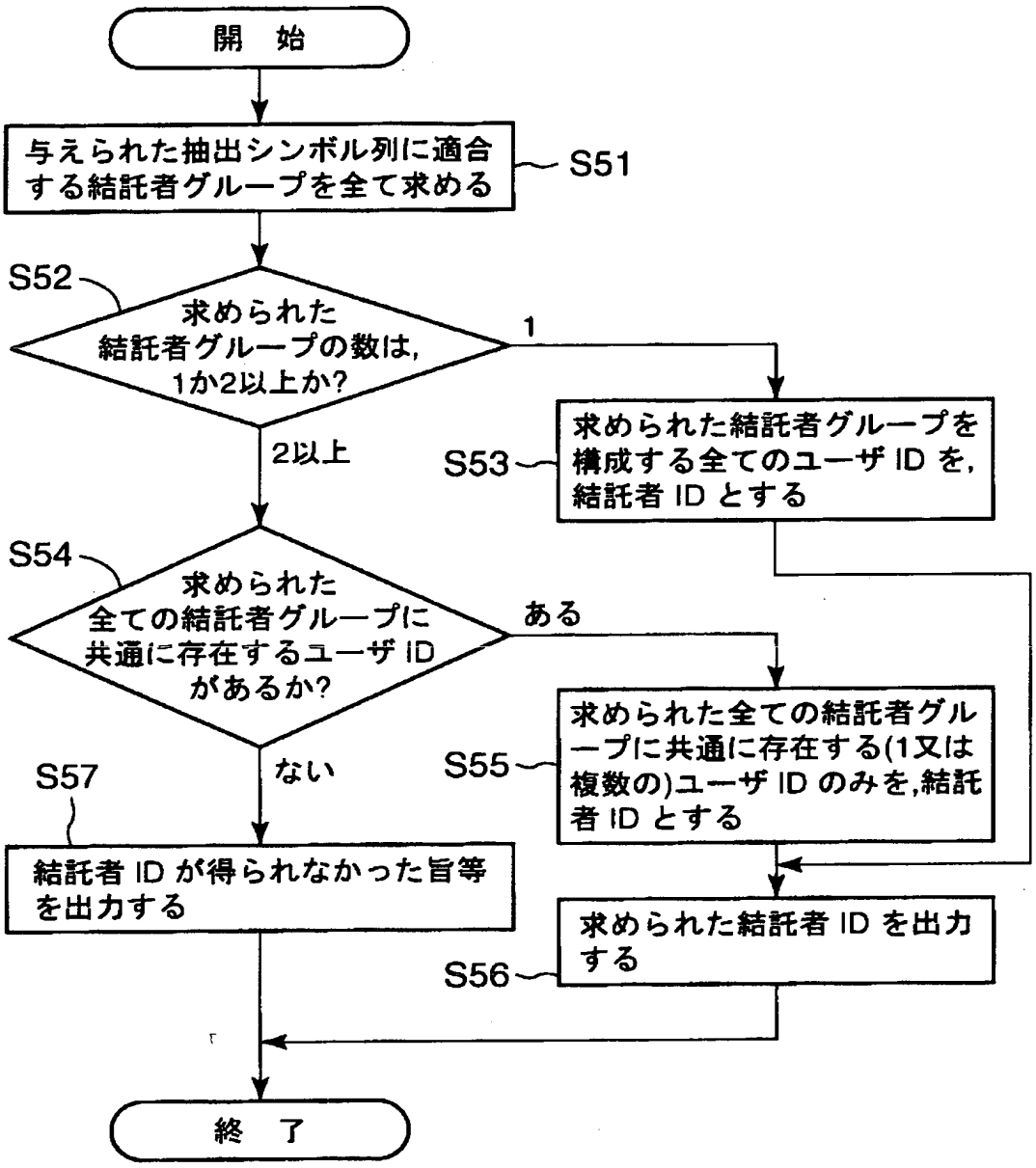
【図１１】


(53/100)
a1,1
最大人口のシンボル
a1,2(26/100)
(a)
a1,4
(13/100)
a1,3(8/100)
a1,1(98/100)
(b)
a1,3(2/100)
a1,1(100/100)
(c)

【図１２】


開　始
S41
全てのユーザ ID (=u) について, D(u) を計算する
S42
D(u) に基づいて,結託者のユーザ ID を特定する
終　了

【図１３】


開　始
与えられた抽出シンボル列に適合する結託者グループを全て求める
S51
S52
求められた結託者グループの数は，1か2以上か?
1
2以上
S53
求められた結託者グループを構成する全てのユーザ ID を，結託者 ID とする
S54
求められた全ての結託者グループに共通に存在するユーザ ID があるか?
ある
ない
S55
求められた全ての結託者グループに共通に存在する(1又は複数の)ユーザ ID のみを，結託者 ID とする
S57
結託者 ID が得られなかった旨等を出力する
求められた結託者 ID を出力する
S56
終　了

【書類名】　　要約書

【要約】

【課題】　結託攻撃に用いられたコンテンツの複製物に埋め込まれていたであろう識別情報を、より感度の高い符号によって推定可能とした電子透かし解析装置を提供すること。

【解決手段】　電子透かし解析装置２は、まず、デジタルコンテンツの複製物から、序列を持った複数の埋め込み符号をそれぞれ抽出する。次いで、抽出された複数の埋め込み符号にそれぞれ対応するシンボルを求め、求められた複数のシンボル列を、対応する埋め込み符号の序列に従って並べてシンボル列を求める。そして、結託攻撃に用いられたデジタルコンテンツの複製物から抽出されたシンボル列及び各々の正当な識別情報に対してそれぞれ一意に割り当てられるシンボル列に基づいて、結託攻撃に用いられたデジタルコンテンツの複製物に埋め込まれていた識別情報を特定する。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００３０７８〕

１．変更年月日　　２００１年　７月　２日
［変更理由］　住所変更
住　所　　東京都港区芝浦一丁目１番１号
氏　名　　株式会社東芝